XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva

Técnicas avanzadas de descubrimiento y análisis de la Dark Net

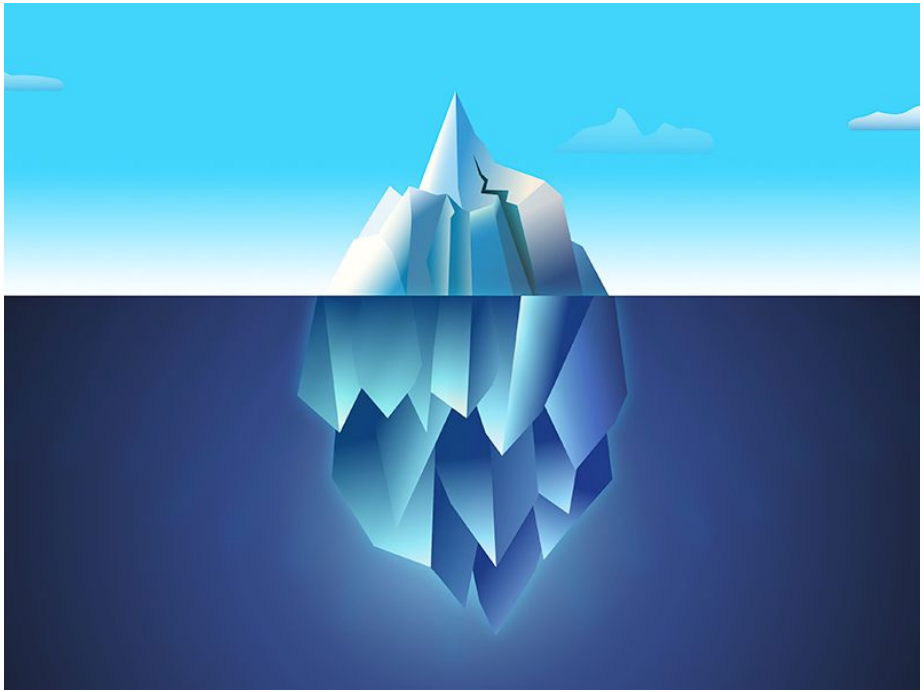
centro criptológico nacional

- Javier Junquera Sánchez
- Personal Investigador (Universidad de Alcalá)
- javier@junquera.xyz

Índice

Introducción

¿Qué es la Dark Net? Internet

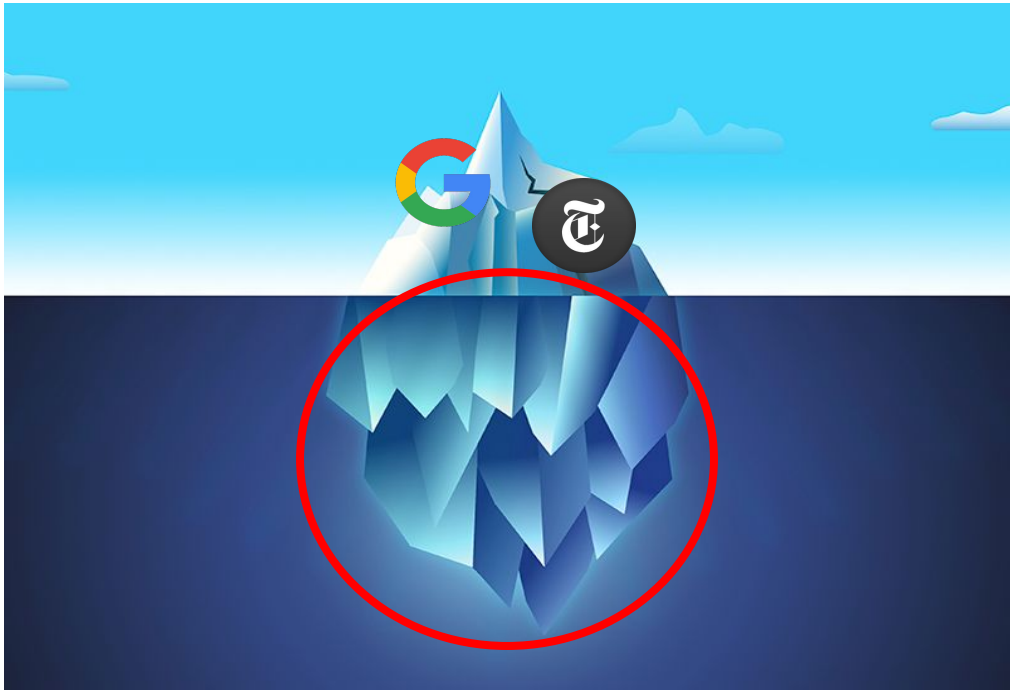


Introducción

¿Qué es la Dark Net? Surface web / Clear net

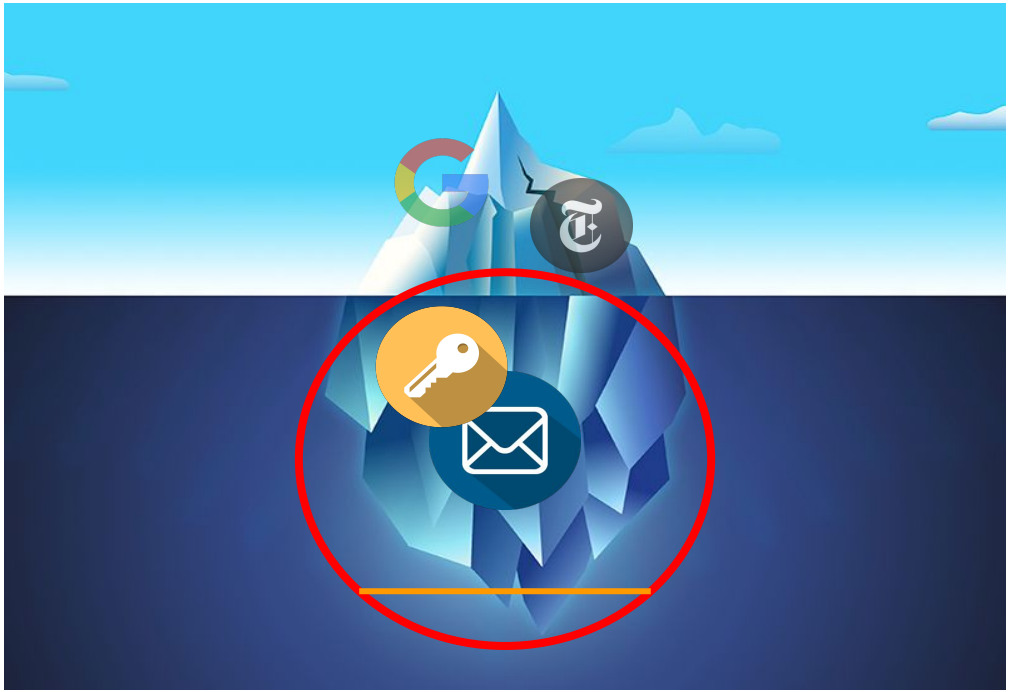
Introducción

¿Qué es la Dark Net? Deep web



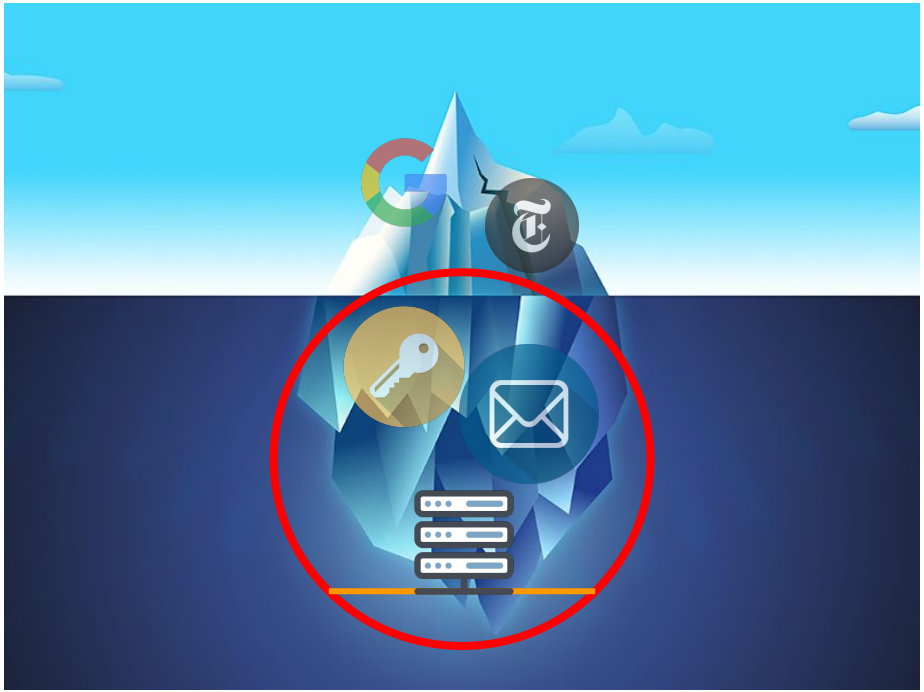
Introducción

¿Qué es la Dark Net? Deep web



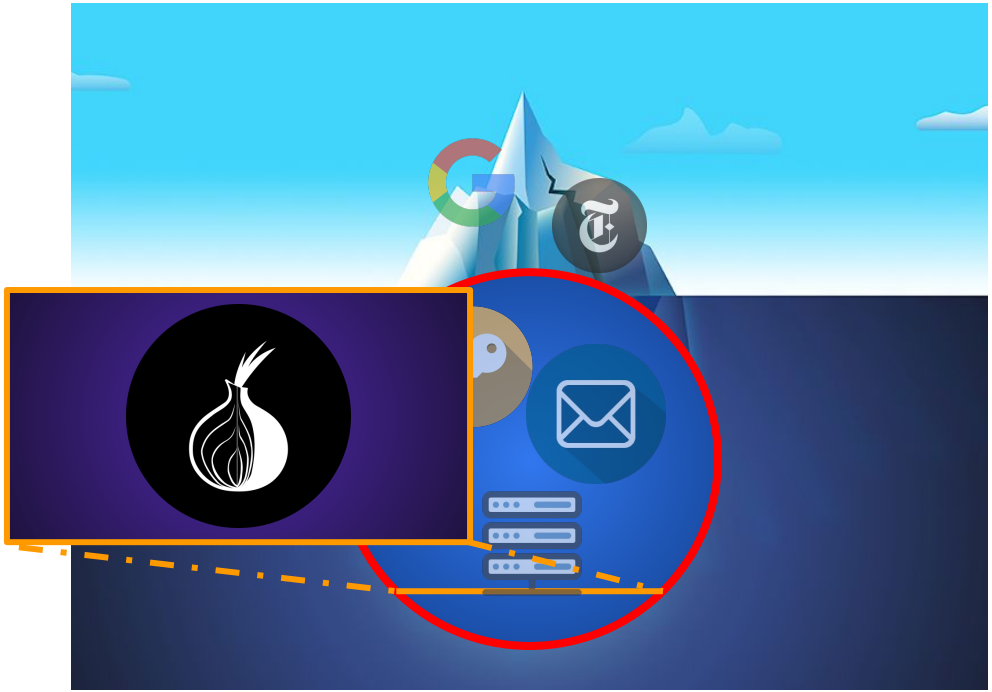
Introducción

¿Qué es la Dark Net? Deep net



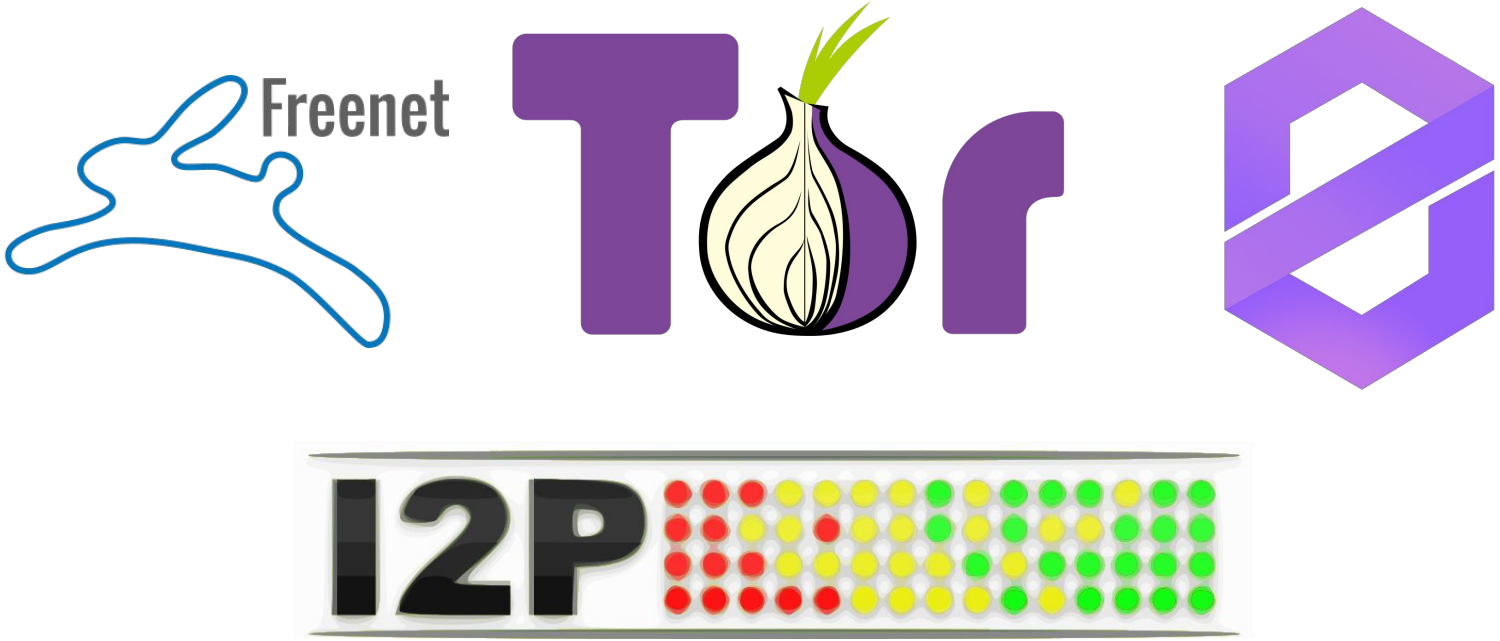
Introducción

¿Qué es la Dark Net? Dark net



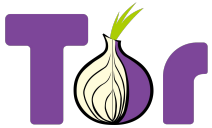
Introducción

Principales Dark Nets



Introducción

Principales Dark Nets

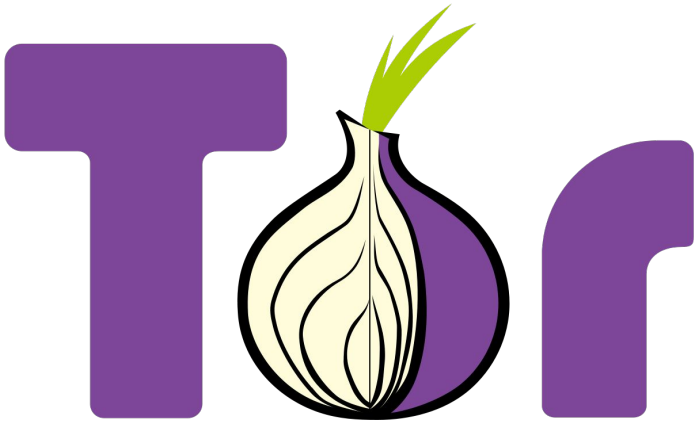


- .onion
- .i2p
- .bit
- freenet: [hash]

Introducción

Principales Dark Nets: Tor

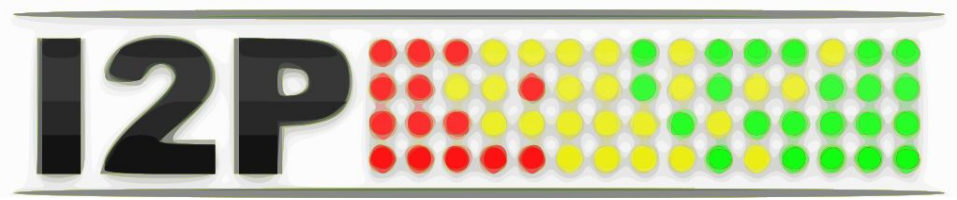
- Enrutado cebolla
- In/Out proxy
- Busca anonimato
- Asequible para novatos



Introducción

Principales Dark Nets: I2P

- Enrutado tipo ajo: mezcla onion con múltiples sub paquetes
- In proxy
- Basado en reputación/agenda



Introducción

Principales Dark Nets: ZeroNet

- Sistema p2p
- Resolución de nombre basada en Namecoin
  - https://namecoin.org/
- Contenido dinámico
- Permite integración con Tor

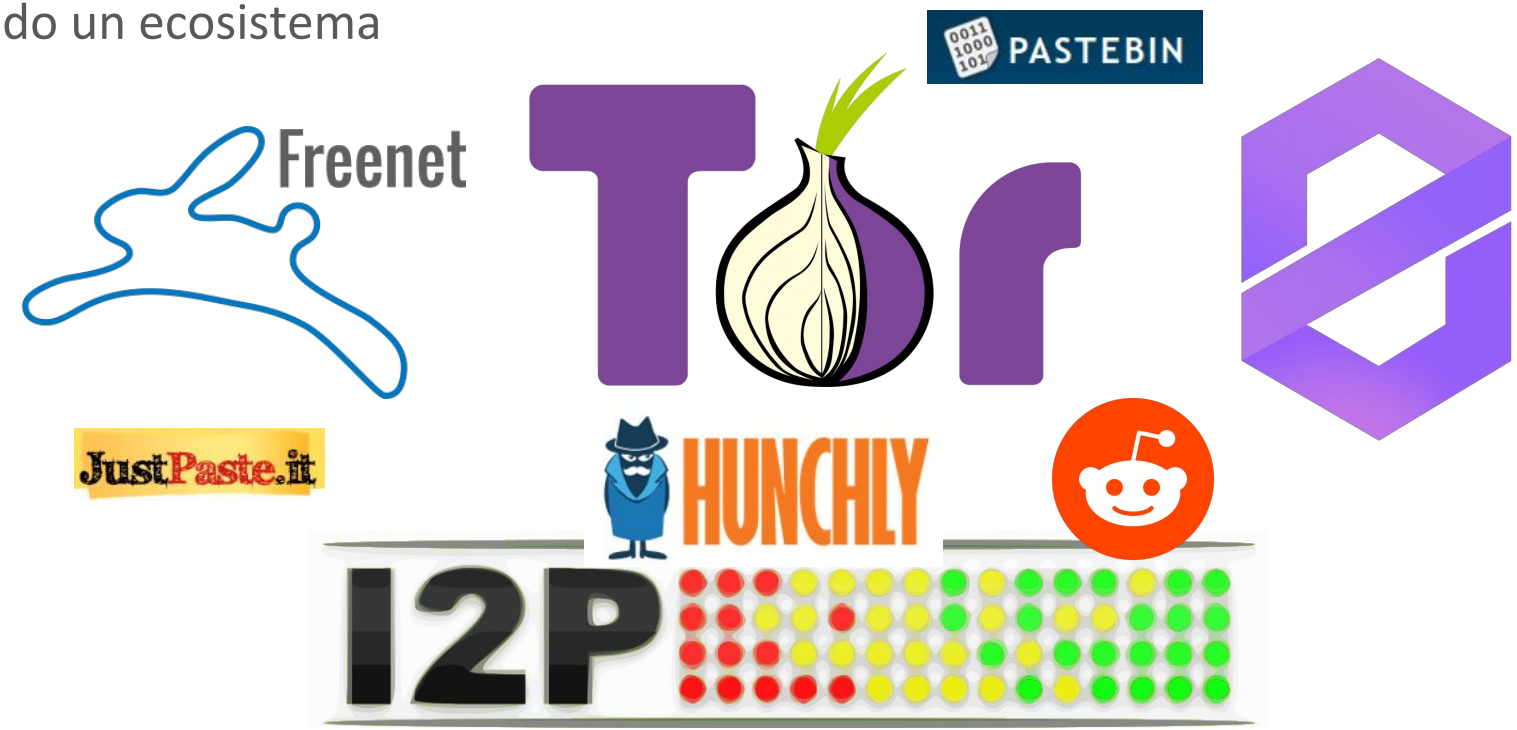
Introducción

Principales Dark Nets: Freenet

- Sistema p2p
- Enrutamiento similar a I2P
- Incensurable
- Al formar parte de la red compartes contenido

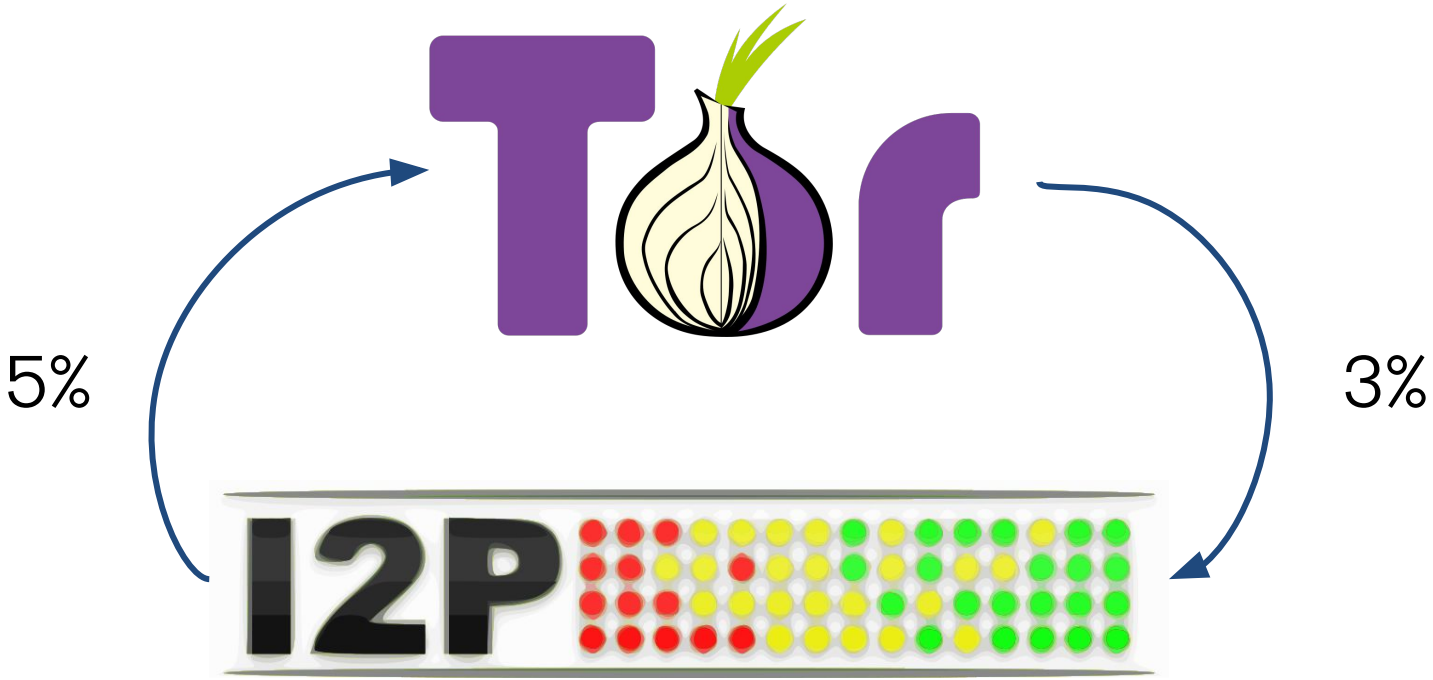
Introducción

Todo un ecosistema



Introducción

Flujo entre redes



Tor

La columna vertebral

- Mantenido por Tor Project, vela por la protección de la privacidad
- Gestiona multitud de proyectos
  - Stem
  - Tails
  - Tor Browser
- Su tecnología sirve de base para otras redes

Tor

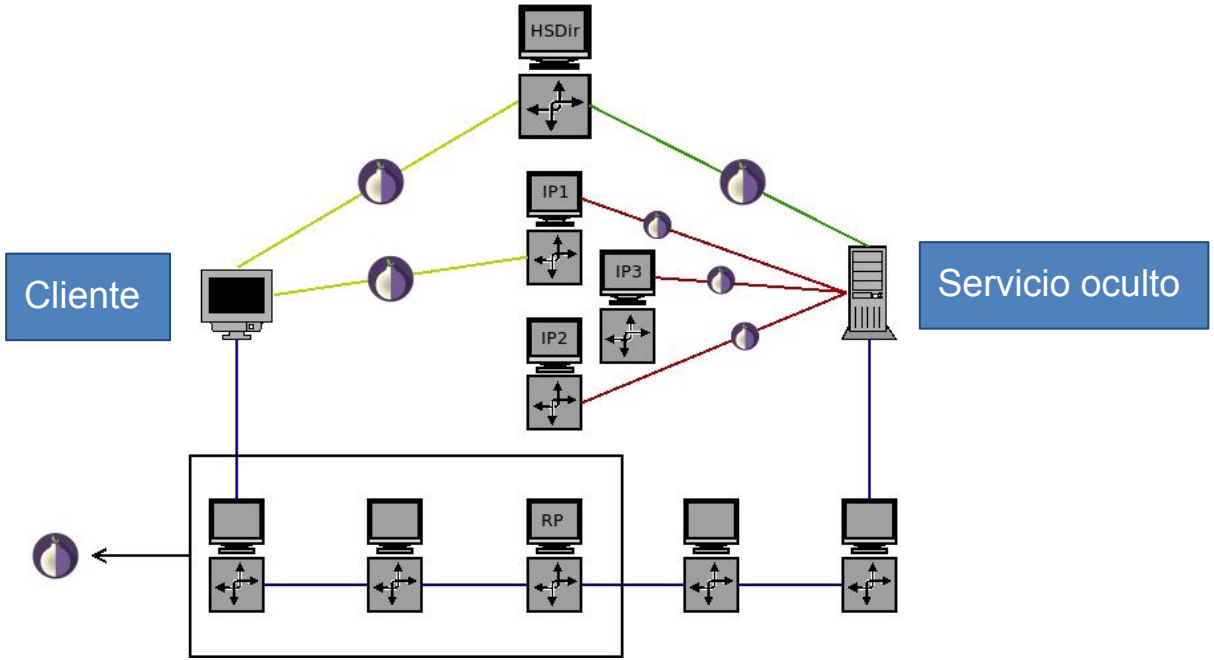
Servicios ocultos

- Una de los principales elementos diferenciadores de Tor es su modo out-proxy
  - Pero nuestro objetivo consiste en conocer la red

- En el modo in-proxy de Tor la funcionalidad la ofrecen los *Hidden Services*
- Su dirección es desconocida para todo el mundo hasta que el administrador del servicio la hace pública

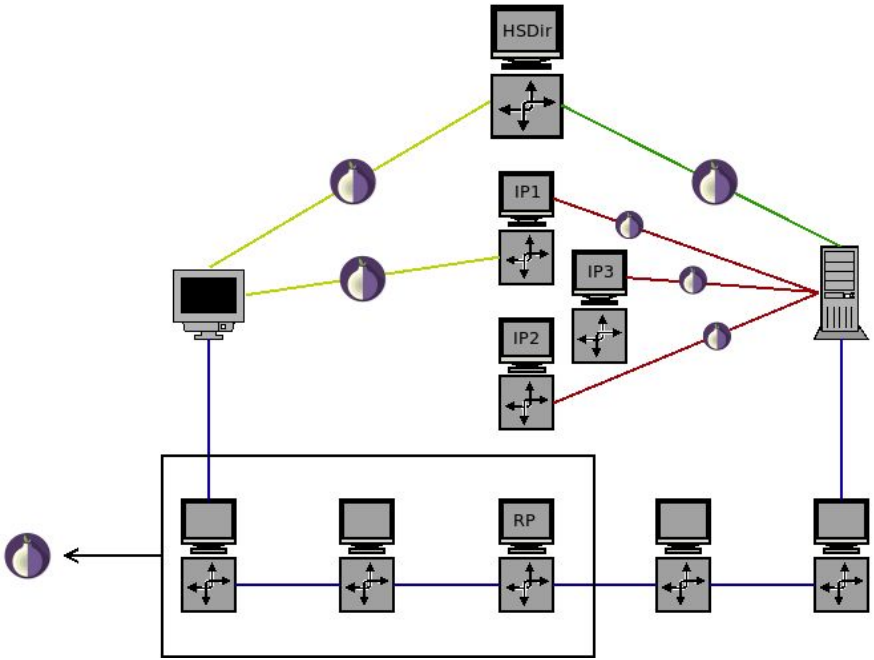
Tor

¿Cómo funciona?



Tor

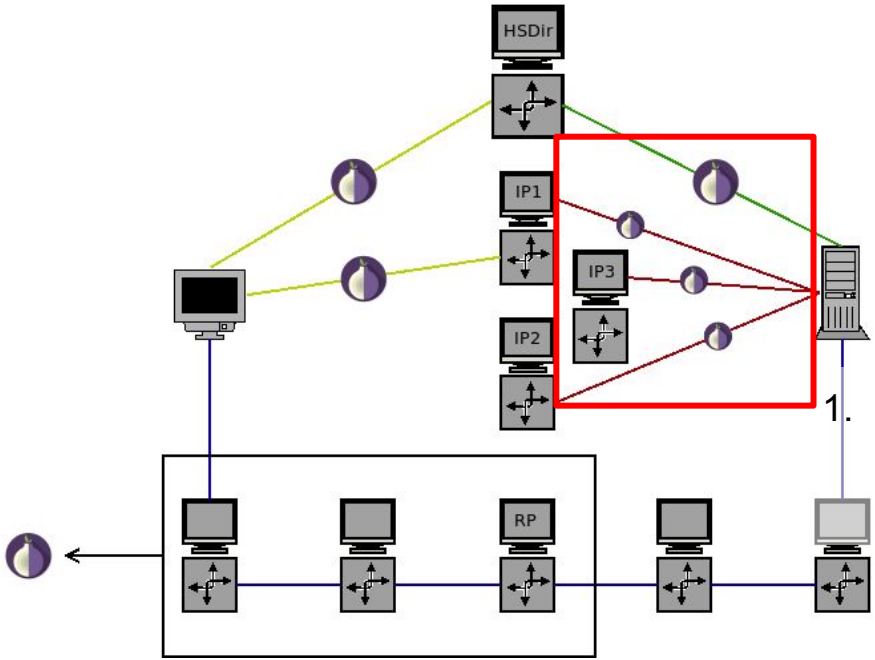
¿Cómo funciona?



Los dominios de los servicios de Tor, por la construcción de la red, son desconocidos si no los publica su dueño

Tor

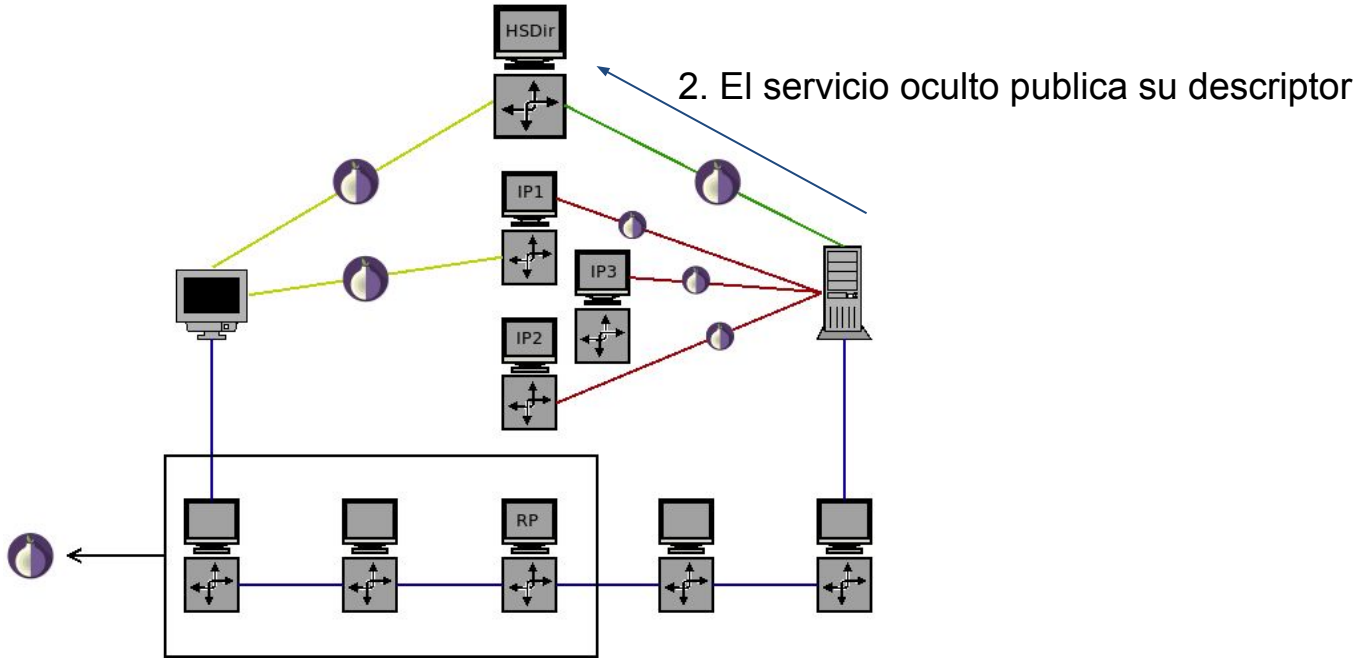
¿Cómo funciona?



1. El servicio oculto contacta con varios equipos

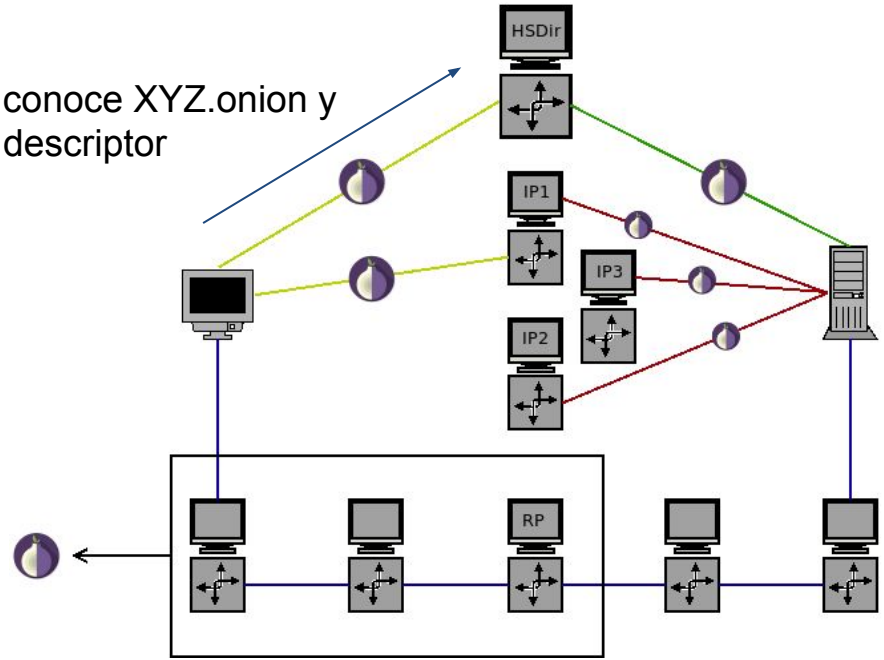
Tor

¿Cómo funciona?

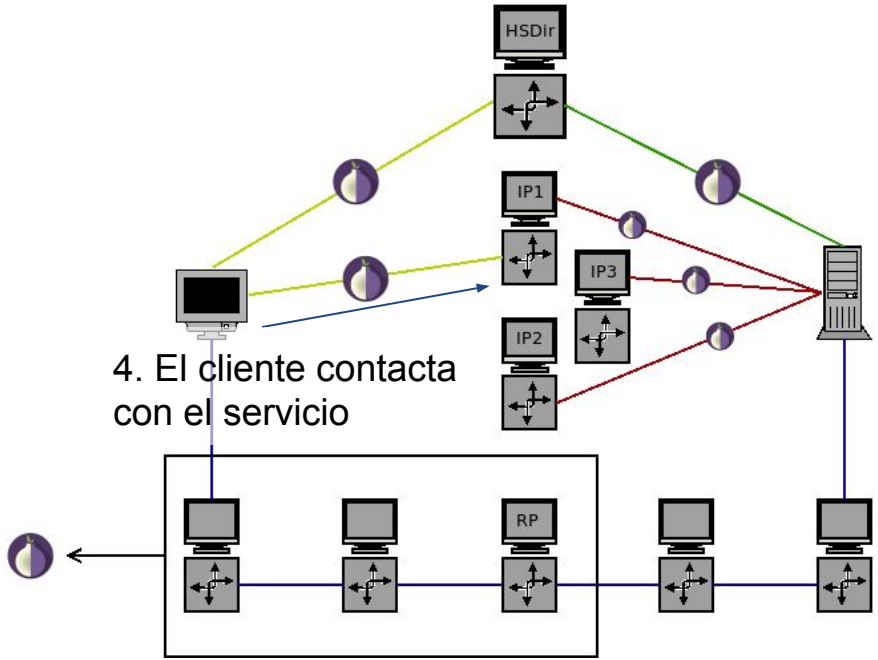


¿Cómo funciona?

3. El cliente conoce XYZ.onion y descarga el descriptor

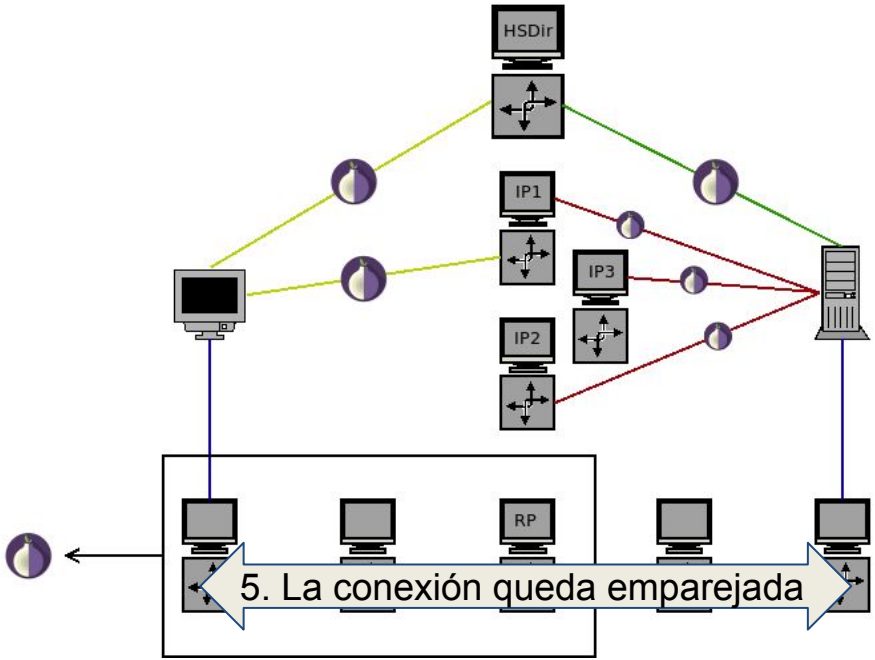


¿Cómo funciona?



Tor

¿Cómo funciona?



Tor

Elementos interesantes

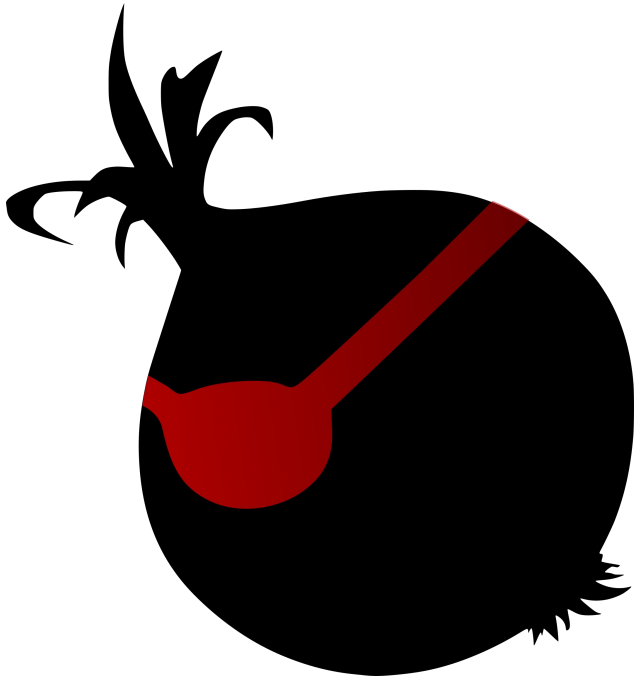
- **HSDir**
  - Directorio en el que se almacenan los descriptores de los servicios ocultos

- **Guard node**
  - Primer nodo al que se conecta la máquina en un enrutamiento a través de Tor

Proyecto Parche

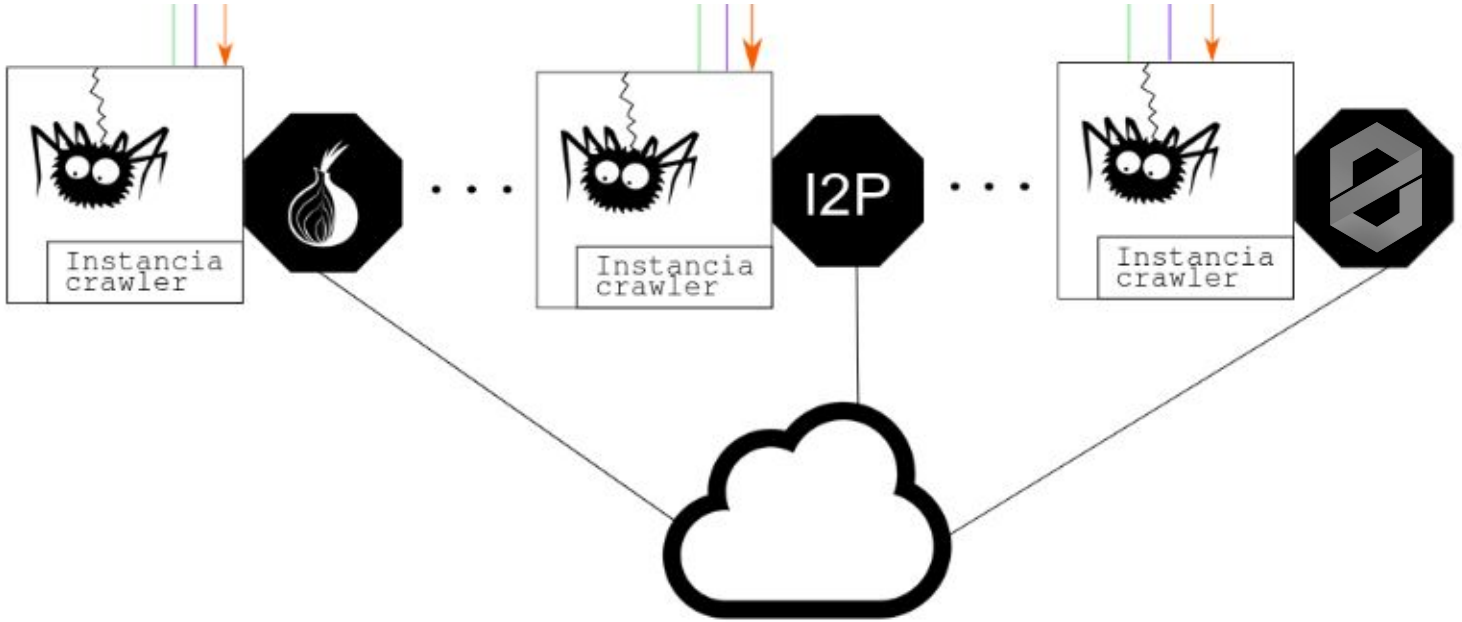
Módulos

- Crawler
  - Tor
  - I2P
  - ZeroNet
- Fuentes abiertas
- Patrones
- Chalota
- Nodo



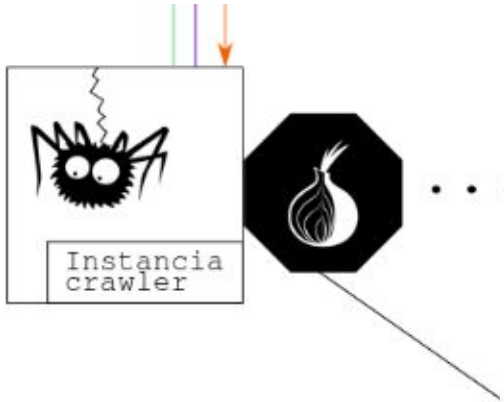
Proyecto Parche

Crawler



Proyecto Parche

Crawler

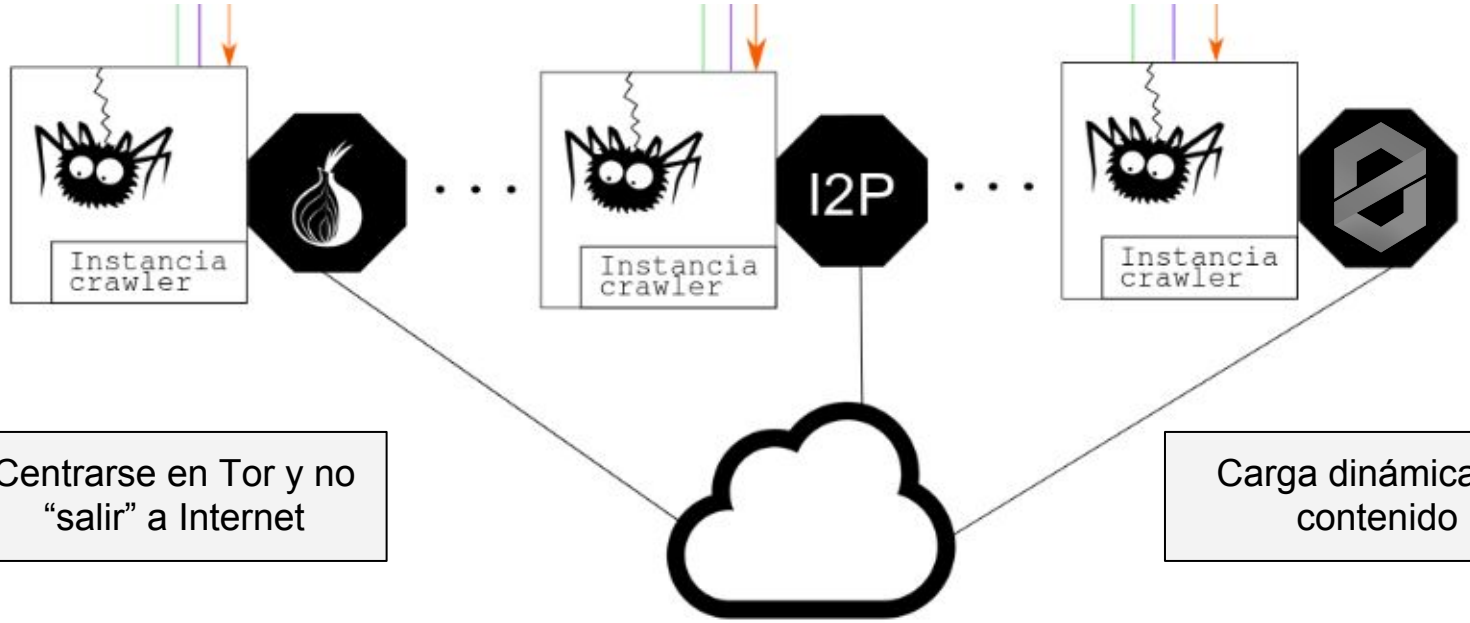


- Tenía que cumplir varios requisitos:
  - Ser distribuible (pocos recursos)
  - Ser reutilizable
  - Ser alimentable

Proyecto Parche

Crawler (dificultades)

Protocolo de descubrimiento

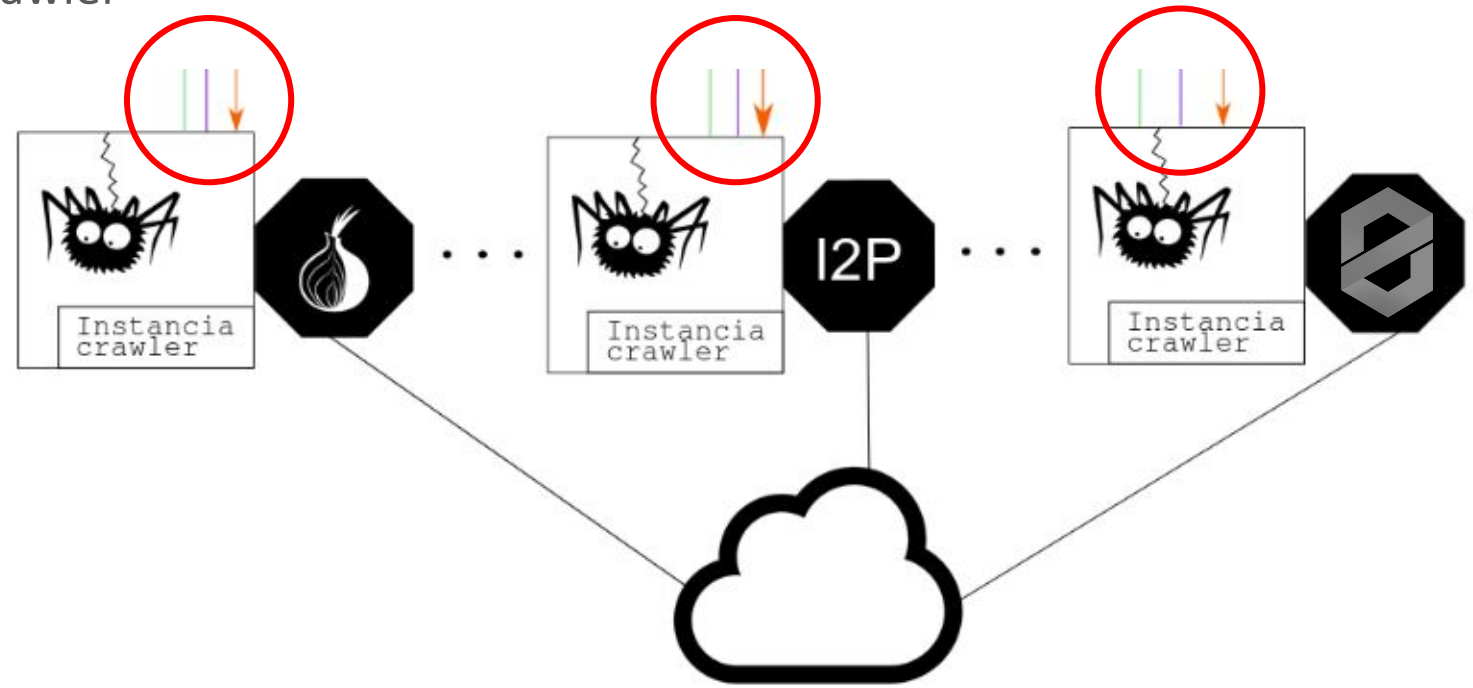


Centrarse en Tor y no "salir" a Internet

Carga dinámica del contenido

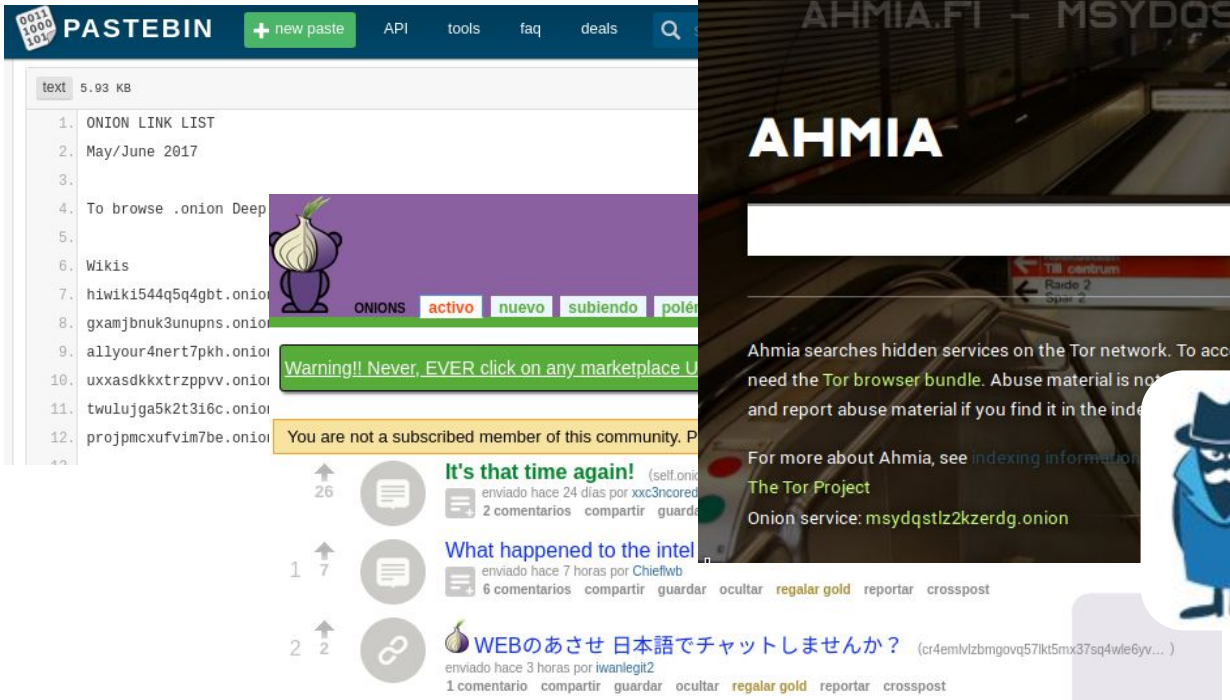
Proyecto Parche

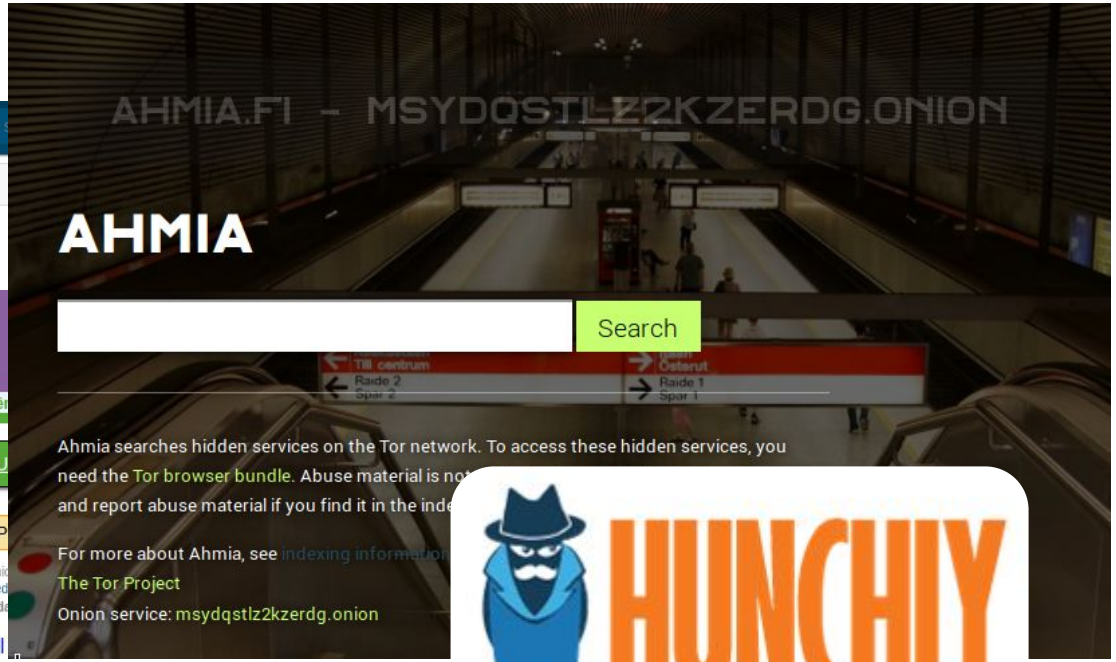
Crawler



Proyecto Parche

Fuentes abiertas





Proyecto Parche

Patrones

- Los dominios *.onion* se generan como un hash de la clave RSA del Hidden Service

```
base32( sha1( PUBKEY ) )[:16]
```

Proyecto Parche

Patrones

- Si quisiéramos encontrar todos los Hidden Services posibles

32^16

=

1208925819614629174706176

Proyecto Parche

Patrones

- Es posible generar un onion a nuestro gusto
  - https://github.com/lachesis/scallion
  - facebookcorewwwi.onion

- Hay webs que fuerzan patrones y podemos buscar en base a estos
  - drmarketcie6vdos.onion
  - epicmarketbbhhmm.onion
  - xmarket334dtd4la.onion

Proyecto Parche

Patrones

- chan
  - 1.152.921.504.606.846.976 dominios
- drugs
  - 36.028.797.018.963.968 dominios
- weapons
  - 35.184.372.088.832 dominios

Proyecto Parche

Búsqueda de patrones

- Análisis de los términos más utilizados en los dominios conocidos
- Generación de listas

	A	B	C
7	2222222222	802	10
33	jzp4uxunl2	256	10
83	zp4uxunl2r	128	10
84	p4uxunl2r5	128	10
85	4uxunl2r5h	128	10
86	uxunl2r5hg	128	10
282	2222222223	38	10
361	xunl2r5hgw	32	10
362	xunl2r5hgx	32	10
363	xunl2r5hgy	32	10
364	xunl2r5hgz	32	10
365	2222222224	32	10
366	2222222225	32	10
873	lolikaastb	14	10
874	jocctilmpo	14	10
1246	kitsune6uv	11	10
1365	libertygb2	10	10
1366	kitsunemkg	10	10
1646	xxxxxxxxxx	9	10

Proyecto Parche

Patrones

```
lolikaastbaakiyk
lolikaastbaakiyl
lolikaastbaakiym
lolikaastbaakiyn
lolikaastbaakiyo
lolikaastbaakiyp
lolikaastbaakiyq
lolikaastbaakiyr
lolikaastbaakiys
lolikaastbaakiyt
lolikaastbaakiyu
lolikaastbaakiyv
lolikaastbaakiyw
lolikaastbaakiyx
lolikaastbaakiyy
lolikaastbaakiyz
lolikaastbaakiy2
lolikaastbaakiy3
lolikaastbaakiy4
lolikaastbaakiy5
lolikaastbaakiy6
lolikaastbaakiy7
```

Proyecto Parche

Chalota

- Necesidad de comprobar eficientemente si un .onion está registrado
  - Uso de sockets y HSFETCH

Proyecto Parche

Tiempos

- Conexión HTTP a través de Tor
  - > 4 segundos
  - ¡Falsos negativos!

```
GET http://facebookcorewwwi.onion
```

- Utilizando protocolo de control Tor
  - < 2 segundos
  - Detección de servicio no web
    - SSH, IRC, FTP

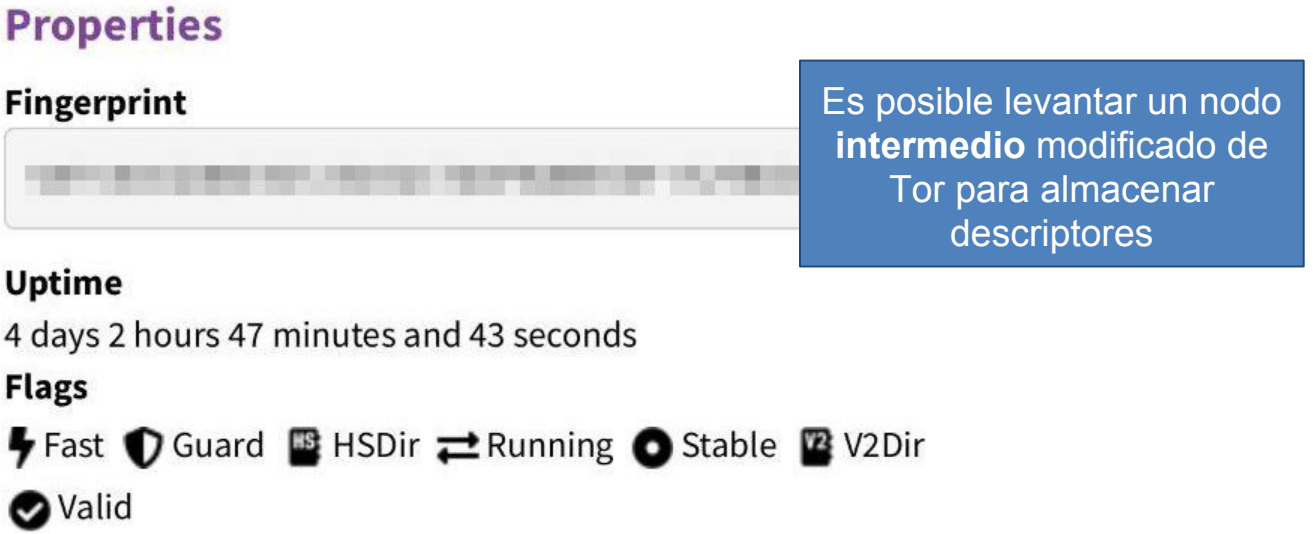
```
AUTHENTICATE "pass"

SETEVENTS HS_DESC

HS_FETCH facebookcorewwwi
```

Proyecto Parche

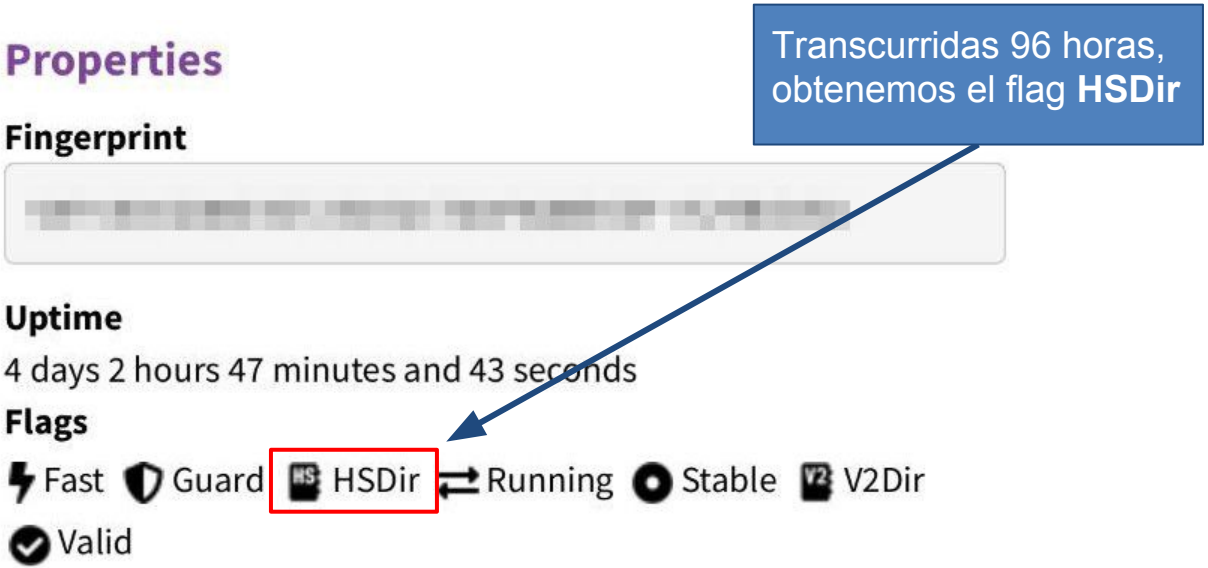
Nodo



Es posible levantar un nodo **intermedio** modificado de Tor para almacenar descriptores

Proyecto Parche

Nodo



Proyecto Parche

Nodo

- Desde el nodo obtenemos las claves RSA
- Con el algoritmo, generamos el nombre del dominio
- Mediante el módulo de comprobación, podemos verificar rápidamente que es correcto

Proyecto Parche

Nodo

```
430B9AC857B7677D0A315A918298.z


log: url: /tor/keys/fp/585769C78764D58426B8B52B6651A5A71137189A+80550987E1D626E3EBA5E5E75A458DE0626D088C
log: headers: GET /tor/keys/fp/585769C78764D58426B8B52B6651A5A71137189A+80550987E1D626E3EBA5E5E75A458DE0626D088


log: url: /tor/rendezvous2/tkemhfcnkwrpkrgkcoo4pk532bp5yaw7
log: headers: GET /tor/rendezvous2/tkemhfcnkwrpkrgkcoo4pk532bp5yaw7 HTTP/1.0


-----BEGIN RSA PUBLIC KEY-----
MIGLAoGBAL6t+Z0pluUT8/4TrqfiQxs/sUFFqt3pebUFjjBzoaT8yAHWFzAEnZ6T
7yI7klB/UF/uPE1KxjV+GHv0458v35wG7YyHM/xSviWfl5rwKGkETSZ2kxedBJzw
cHBu1c8AsioZMdDF/49piExfj4VVD4eouJZ7o1/KLypjRcRFYf6hAgUCAPcqKw==
-----END RSA PUBLIC KEY-----

log: (null)
log: d/1FA28F9BD8B72146D44F87FCC97EA32A4062D337+216F6677DE44D6FEAA5C05E792F6FDA79657E1B5+D896E0B2F9EFEF124A0BFE
430B9AC857B7677D0A315A918298.z
log: url: /tor/keys/fp/27B6B5996C426270A5C95488AA5BCEB6BCC86956+585769C78764D58426B8B52B6651A5A71137189A+805509
88C
log: headers: GET /tor/keys/fp/27B6B5996C426270A5C95488AA5BCEB6BCC86956+585769C78764D58426B8B52B6651A5A7113718
DE0626D088C HTTP/1.0
Host: 141.145.121.11:9001


log: (null)
log: ????^A>??ŏ?U`^O^ ?^6?60
log: (null)
```

Proyecto Parche

Nodo

```
430B9AC857B7677D0A315A918298.z


log: url: /tor/keys/fp/585769C78764D58426B8B52B6651A5A71137189A+80550987E1D626E3EBA5E5E75A458DE0626D088C
log: headers: GET /tor/keys/fp/585769C78764D58426B8B52B6651A5A71137189A+80550987E1D626E3EBA5E5E75A458DE0626D088


log: url: /tor/rendezvous2/tkemhfcnkwrpkrgkcoo4pk532bp5yaw7
log: headers: GET /tor/rendezvous2/tkemhfcnkwrpkrgkcoo4pk532bp5yaw7 HTTP/1.0


-----BEGIN RSA PUBLIC KEY-----
MIGLAoGBAL6t+Z0pluUT8/4TrqfiQxs/sUFFqt3pebUFjjBzoaT8yAHWFzAEnZ6T
7yI7klB/UF/uPE1KxjV+GHv0458v35wG7YyHM/xSviWfl5rwKGkETSZ2kxedBJzw
cHBu1c8AsioZMdDF/49piExfj4VVD4eouJZ7o1/KLypjRcRFYf6hAgUCAPcqKw==
-----END RSA PUBLIC KEY-----

log: (null)
log: d/1FA28F9BD8B72146D44F87FCC97EA32A4062D337+216F6677DE44D6FEAA5C05E792F6FDA79657E1B5+D896E0B2F9EFEF124A0BFE
430B9AC857B7677D0A315A918298.z
log: url: /tor/keys/fp/27B6B5996C426270A5C95488AA5BCEB6BCC86956+585769C78764D58426B8B52B6651A5A71137189A+805509
88C
log: headers: GET /tor/keys/fp/27B6B5996C426270A5C95488AA5BCEB6BCC86956+585769C78764D58426B8B52B6651A5A7113718
DE0626D088C HTTP/1.0
Host: 141.145.121.11:9001


log: (null)
log: ????^A>??ŏ?U`^O^ ?^6?60
log: (null)
```

Proyecto Parche

Nodo

- Extraemos la clave pública del descriptor

```
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAPLSSLvEPG6PtXnGBfkkNZ6NxzRNSVh3Ph3ADcGVfcFf0krgZdqT
ok4g
e66ZzlXVfP1MsDYpk2ZNPN2W3wB7iLU9RGTK05xIw/y7Z6BPEZiZ5FsxWrVC
Pyma
gnNRA0urAZJWIdBRB0wxqs2Eunz7utSrYyxb7mCh5B5F+RU44xMrAgMBAAE=
-----END RSA PUBLIC KEY-----
```

Proyecto Parche

Nodo

- Gracias a la clave pública podemos obtener el .onion

```
-----BEGIN RSA PUBLIC KEY-----
7gheeonpk6bqfkdi
-----END RSA PUBLIC KEY-----
```

Proyecto Parche

Nodo

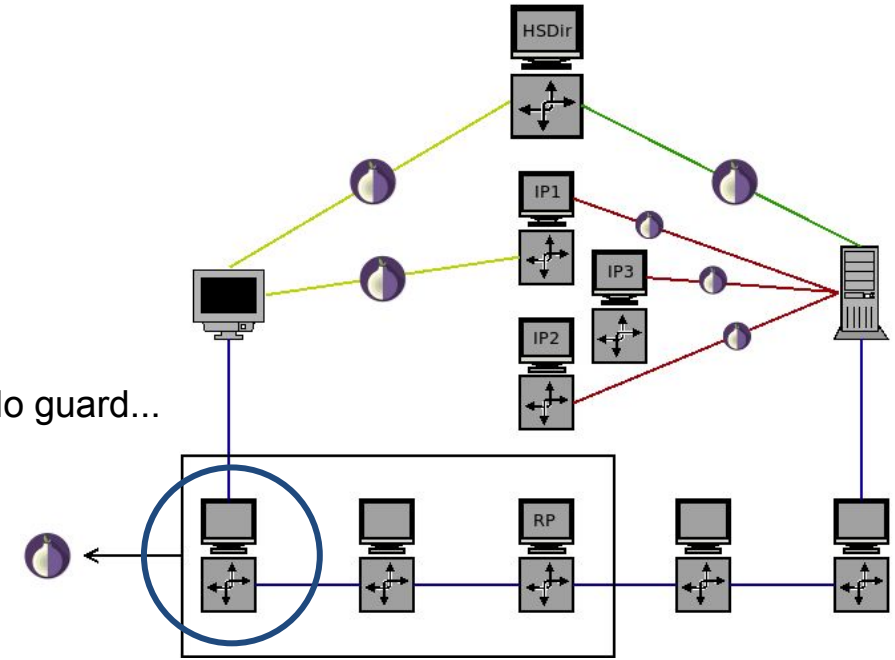
- Tor tiene mecanismos para detectar exfiltración de dominios
  - Hay que desarrollar técnicas para evitar baneos

- La solución deja de ser viable en la versión 3 de Tor
  - Hay que investigar nuevos métodos

Proyecto Parche

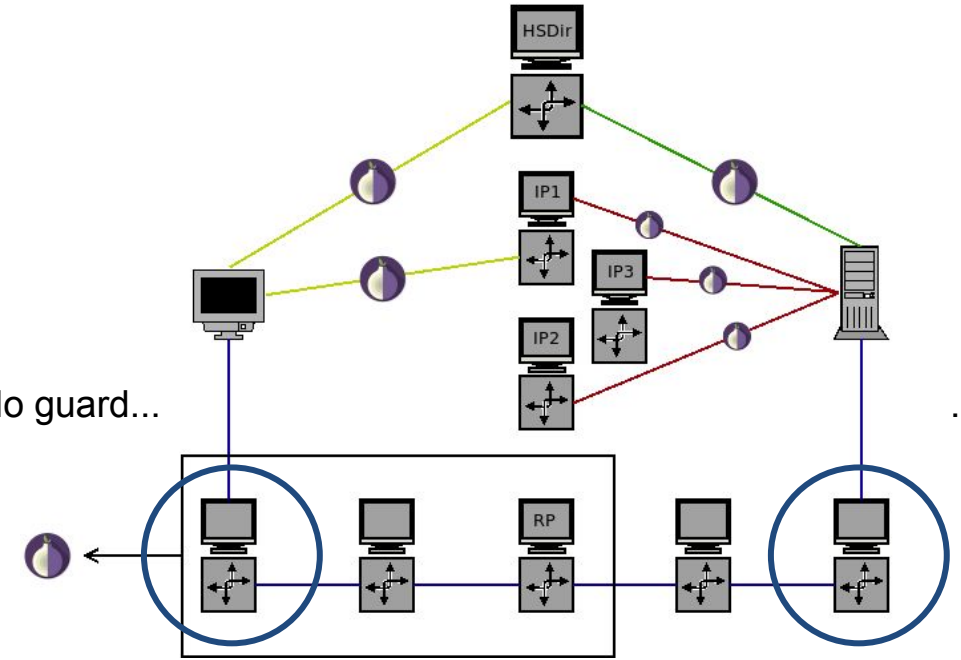
Nodo

Este es un nodo guard...



Proyecto Parche

Nodo



Este es un nodo guard...

… pero este también

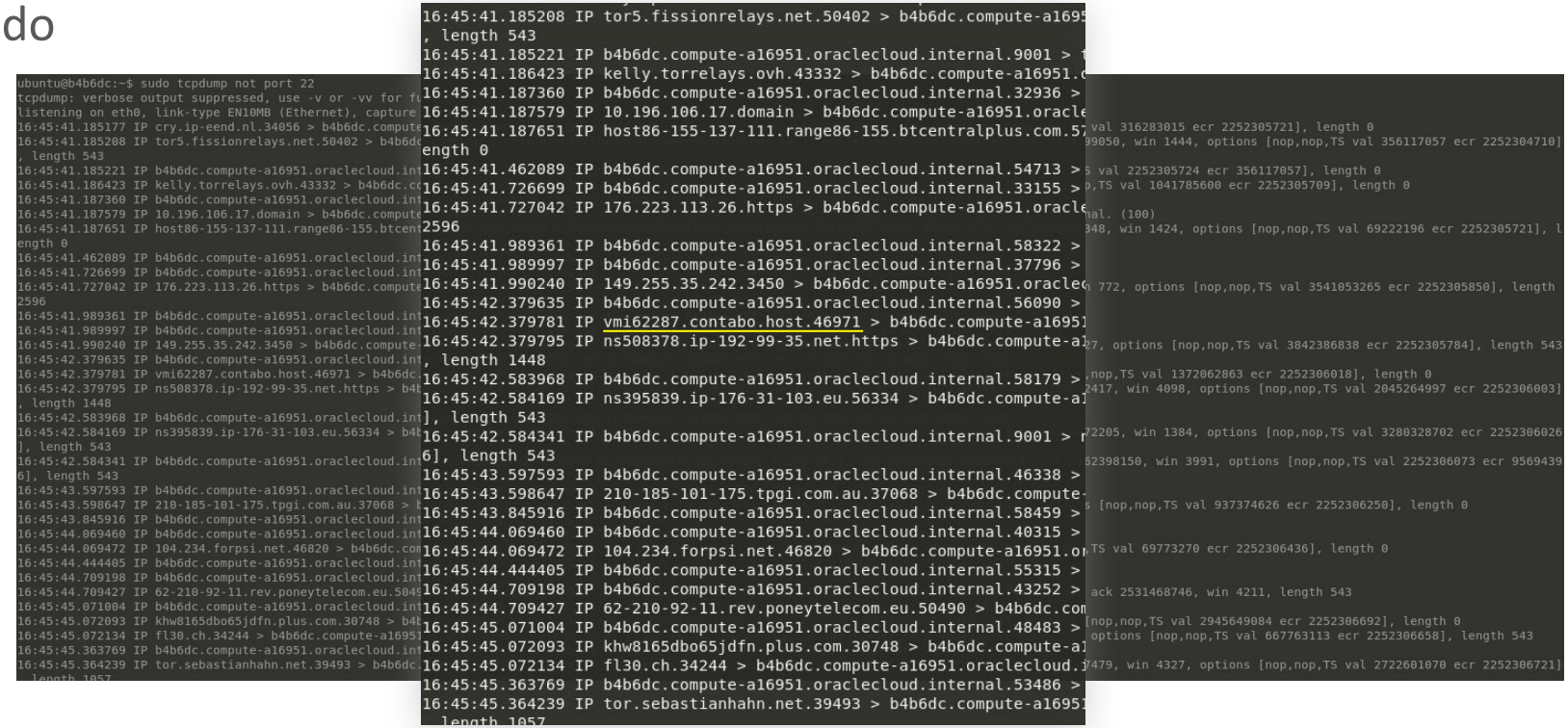
Proyecto Parche

Nodo

```
ubuntu@b4b6dc:~$ sudo tcpdump not port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:45:41.185177 IP cry.ip-eend.nl.34056 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [.], ack 4185503583, win 1773, options [nop,nop,TS val 316283015 ecr 2252305721], length 0
16:45:41.185208 IP tor5.fissionrelays.net.50402 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [P.], seq 4138023973:4138024516, ack 2354399050, win 1444, options [nop,nop,TS val 356117057 ecr 2252304710]
, length 543
16:45:41.185221 IP b4b6dc.compute-a16951.oraclecloud.internal.9001 > tor5.fissionrelays.net.50402: Flags [.], ack 543, win 3586, options [nop,nop,TS val 2252305724 ecr 356117057], length 0
16:45:41.186423 IP kelly.torrelays.ovh.43332 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [.], ack 533805795, win 2557, options [nop,nop,TS val 1041785600 ecr 2252305709], length 0
16:45:41.187360 IP b4b6dc.compute-a16951.oraclecloud.internal.32936 > 10.196.106.17.domain: 60404+ PTR? 18.106.196.10.in-addr.arpa. (44)
16:45:41.187579 IP 10.196.106.17.domain > b4b6dc.compute-a16951.oraclecloud.internal.32936: 60404 1/0/0 PTR b4b6dc.compute-a16951.oraclecloud.internal. (100)
16:45:41.187651 IP host86-155-137-111.range86-155.btcentralplus.com.57424 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [.], ack 2582042348, win 1424, options [nop,nop,TS val 69222196 ecr 2252305721], l
ength 0
16:45:41.462089 IP b4b6dc.compute-a16951.oraclecloud.internal.54713 > 10.196.106.17.domain: 2556+ PTR? 154.26.255.51.in-addr.arpa. (44)
16:45:41.726699 IP b4b6dc.compute-a16951.oraclecloud.internal.33155 > 10.196.106.17.domain: 60718+ PTR? 164.229.251.148.in-addr.arpa. (46)
16:45:41.727042 IP 176.223.113.26.https > b4b6dc.compute-a16951.oraclecloud.internal.47959: Flags [.], seq 2800143113:2800145709, ack 326597969, win 772, options [nop,nop,TS val 3541053265 ecr 2252305850], length
2596
16:45:41.989361 IP b4b6dc.compute-a16951.oraclecloud.internal.58322 > 10.196.106.17.domain: 61042+ PTR? 17.106.196.10.in-addr.arpa. (44)
16:45:41.989997 IP b4b6dc.compute-a16951.oraclecloud.internal.37796 > 10.196.106.17.domain: 58411+ PTR? 111.137.155.86.in-addr.arpa. (45)
16:45:41.990240 IP 149.255.35.242.3450 > b4b6dc.compute-a16951.oraclecloud.internal.56379: Flags [P.], seq 20689480:20690023, ack 3465002096, win 727, options [nop,nop,TS val 3842386838 ecr 2252305784], length 543
16:45:42.379635 IP b4b6dc.compute-a16951.oraclecloud.internal.56090 > 10.196.106.17.domain: 41428+ PTR? 26.113.223.176.in-addr.arpa. (45)
16:45:42.379781 IP vmi62287.contabo.host.46971 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [.], ack 4072281848, win 9234, options [nop,nop,TS val 1372062863 ecr 2252306018], length 0
16:45:42.379795 IP ns508378.ip-192-99-35.net.https > b4b6dc.compute-a16951.oraclecloud.internal.60661: Flags [.], seq 74332857:74334305, ack 4228602417, win 4098, options [nop,nop,TS val 2045264997 ecr 2252306003]
, length 1448
16:45:42.583968 IP b4b6dc.compute-a16951.oraclecloud.internal.58179 > 10.196.106.17.domain: 39725+ PTR? 242.35.255.149.in-addr.arpa. (45)
16:45:42.584169 IP ns395839.ip-176-31-103.eu.56334 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [P.], seq 972443470:972444013, ack 100872205, win 1384, options [nop,nop,TS val 3280328702 ecr 2252306026
], length 543
16:45:42.584341 IP b4b6dc.compute-a16951.oraclecloud.internal.9001 > ns.km32809-01.keymachine.de.38167: Flags [P.], seq 851351480:851352023, ack 3162398150, win 3991, options [nop,nop,TS val 2252306073 ecr 9569439
6], length 543
16:45:43.597593 IP b4b6dc.compute-a16951.oraclecloud.internal.46338 > 10.196.106.17.domain: 38147+ PTR? 89.81.136.213.in-addr.arpa. (44)
16:45:43.598647 IP 210-185-101-175.tpgi.com.au.37068 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [.], ack 1051809613, win 1440, options [nop,nop,TS val 937374626 ecr 2252306250], length 0
16:45:43.845916 IP b4b6dc.compute-a16951.oraclecloud.internal.58459 > 10.196.106.17.domain: 59397+ PTR? 91.35.99.192.in-addr.arpa. (43)
16:45:44.069460 IP b4b6dc.compute-a16951.oraclecloud.internal.40315 > 10.196.106.17.domain: 45293+ PTR? 150.103.31.176.in-addr.arpa. (45)
16:45:44.069472 IP 104.234.forpsi.net.46820 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [.], ack 593826313, win 4508, options [nop,nop,TS val 69773270 ecr 2252306436], length 0
16:45:44.444405 IP b4b6dc.compute-a16951.oraclecloud.internal.55315 > 10.196.106.17.domain: 36826+ PTR? 120.122.118.87.in-addr.arpa. (45)
16:45:44.709198 IP b4b6dc.compute-a16951.oraclecloud.internal.43252 > 10.196.106.17.domain: 13368+ PTR? 175.101.185.210.in-addr.arpa. (46)
16:45:44.709427 IP 62-210-92-11.rev.poneytelecom.eu.50490 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [P.], seq 1987309193:1987309736, ack 2531468746, win 4211, length 543
16:45:45.071004 IP b4b6dc.compute-a16951.oraclecloud.internal.48483 > 10.196.106.17.domain: 50828+ PTR? 104.234.2.81.in-addr.arpa. (43)
16:45:45.072093 IP khw8165dbo65jdfn.plus.com.30748 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [.], ack 2894523935, win 1444, options [nop,nop,TS val 2945649084 ecr 2252306692], length 0
16:45:45.072134 IP fl30.ch.34244 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [P.], seq 2064734344:2064734887, ack 700394907, win 2352, options [nop,nop,TS val 667763113 ecr 2252306658], length 543
16:45:45.363769 IP b4b6dc.compute-a16951.oraclecloud.internal.53486 > 10.196.106.17.domain: 6534+ PTR? 11.92.210.62.in-addr.arpa. (43)
16:45:45.364239 IP tor.sebastianhahn.net.39493 > b4b6dc.compute-a16951.oraclecloud.internal.9001: Flags [P.], seq 2142915107:2142916164, ack 3500247479, win 4327, options [nop,nop,TS val 2722601070 ecr 2252306721]
, length 1057
```

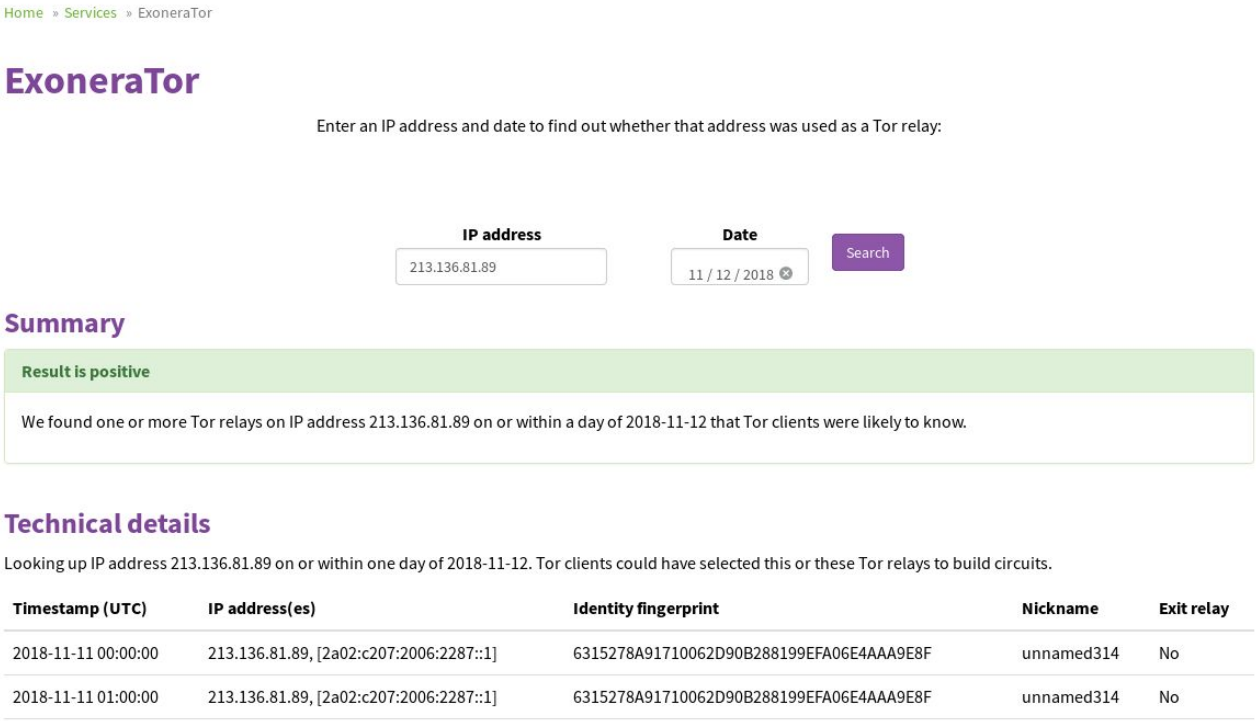
Proyecto Parche

Nodo



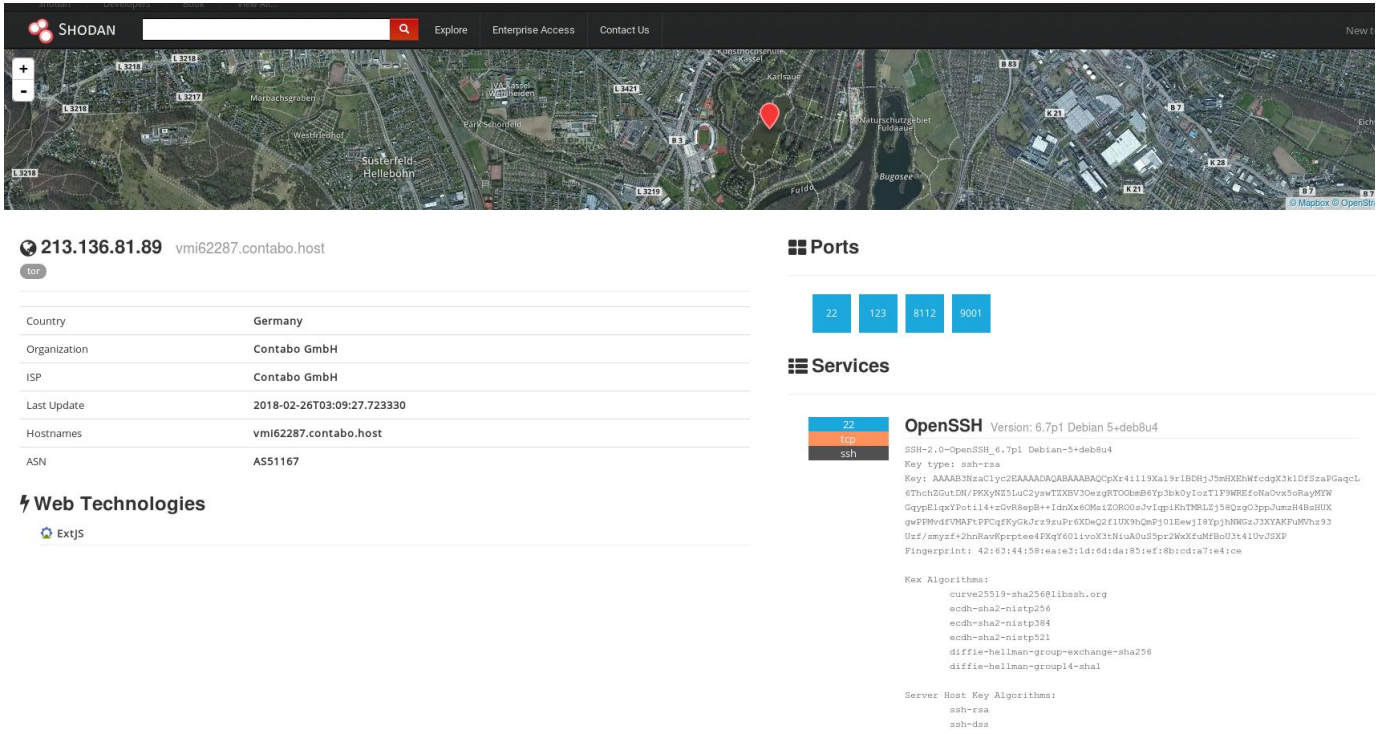
Proyecto Parche

Nodo



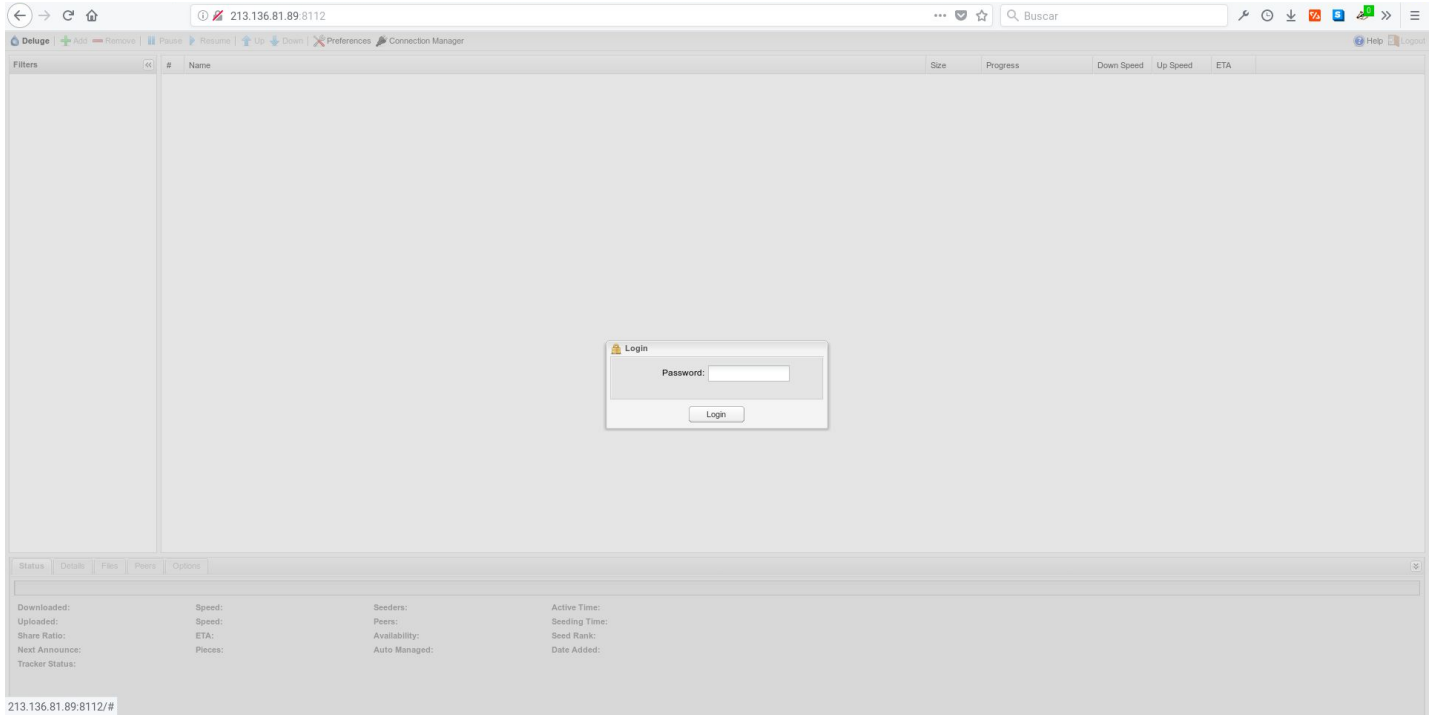
Proyecto Parche

Nodo



Proyecto Parche

Nodo



Proyecto Parche

Estadísticas de datos y análisis

- Detección de idioma
- Detección de temática
- Stalker
  - Detección en base a regex
    - Canales de Telegram, Whatsapp, Discord
    - Direcciones email
    - Direcciones i2p, zeronet, tor
  - https://gitlab.com/junquera/stalker

Proyecto Parche

Estadísticas de datos y análisis

- **BTC Wallet:** 143.299
- **Email:** 74.251
- **tor url:** 28.645.396 (11.657 dominios)
- **i2p url:** 2.208.758 (2.041 dominios)
- **Twitter_username:** 3.176
- **Whatsapp:** 7
- **Canales de Telegram:** 254
- **Teléfonos:** 11.207 (en torno a 376 de España)

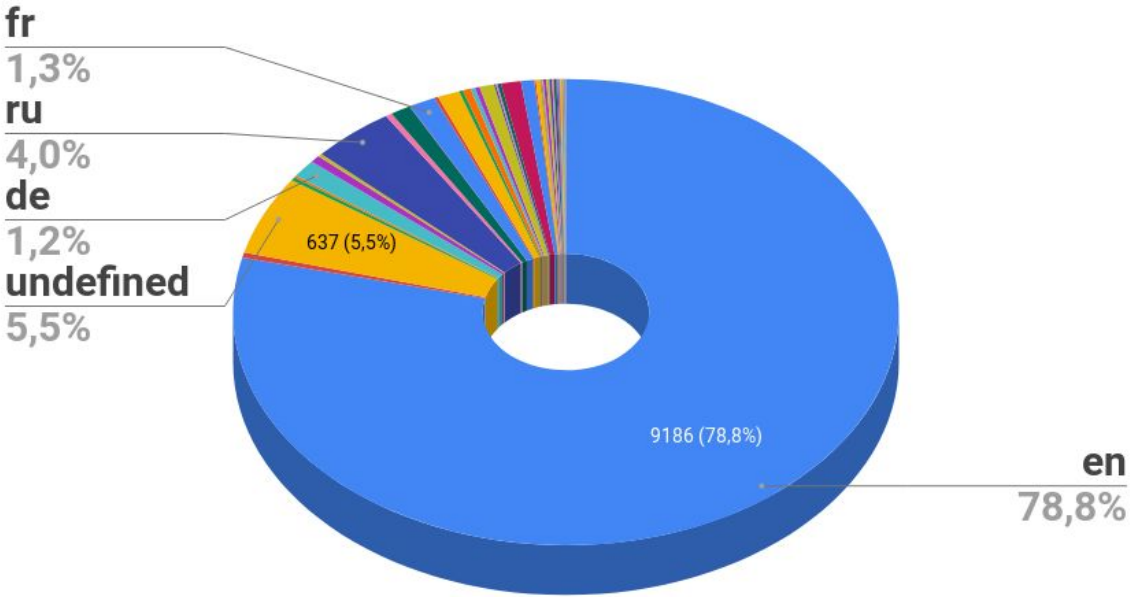
Resultados

Estadísticas de datos y análisis

- Hemos llegado a ver 139.912 dominios *.onion*
  - No todos alojan webs
    - ¡Algunos alojan las instrucciones para acceder a la web!
  - No todos están activos 24/7
  - Chalota permite comprobar rápidamente los servicios

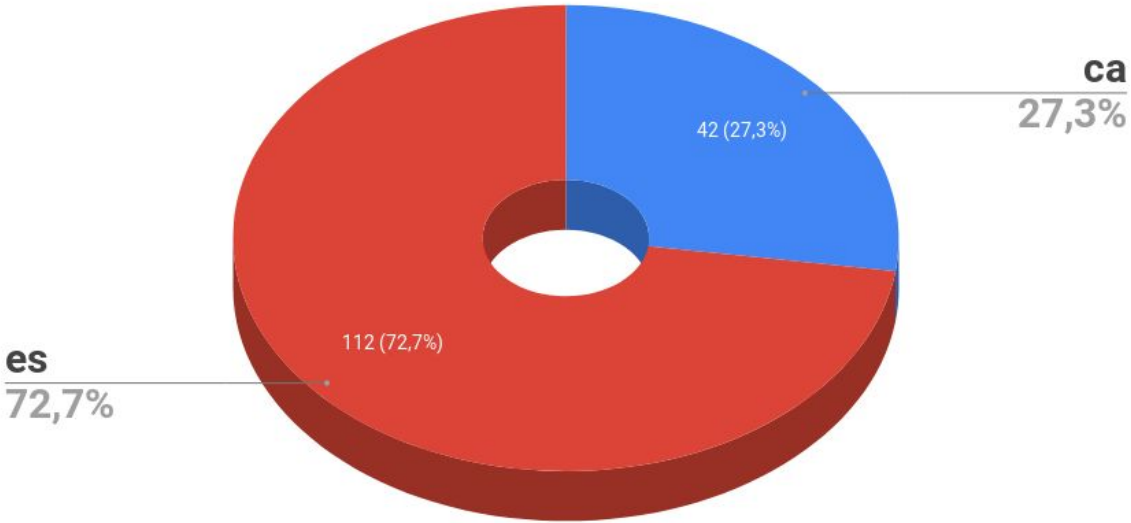
Uso de machine learning

Detección de idioma



Uso de machine learning

Detección de idioma

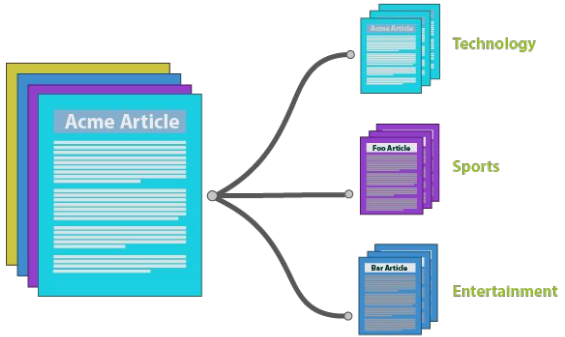


Uso de machine learning

Detección de temática

- Generación de modelo usando 20 Newsgroups
  - Enriquecimiento del dataset usando datos recopilados
  - Nuevas categorías
    - Hitman, Markets, Criptomonedas, Pornografía
    - Posible generar en base a marcas concretas

comp.graphics comp.os.ms-windows.misc comp.sys.ibm.pc.hardware comp.sys.mac.hardware comp.windows.x	rec.autos rec.motorcycles rec.sport.baseball rec.sport.hockey	sci.crypt sci.electronics sci.med sci.space
misc.forsale	talk.politics.misc talk.politics.guns talk.politics.mideast	talk.religion.misc alt.atheism soc.religion.christian



Tor v3

Criptografía de curva elíptica

- En lugar de RSA, la versión 3 de Tor utiliza criptografía de curva elíptica, con la curva **ed25519**
  - Nuevos dominios de 56 caracteres
  - Nuevo sistema de publicación de descriptores

Tor v3

Nuevo formato de direcciones

32zzibxmqi2ybxpqyggwwuwz7a3lbvtzoloti7cxoevyvijexvgsfeid.onion

VERSION = “\x03”

CHECKSUM = sha3_256(".onion checksum" | **PUBKEY** | **VERSION**)[:2]

base32(**PUBKEY** | **CHECKSUM** | **VERSION**)

Tor v3

Nuevo formato de direcciones

1.942.668.892.225.729.070.919.461.
906.823.518.906.642.406.839.052.
139.521.251.812.409.738.904.285.
205.208.498.176 dominios

Tor v3

Nuevo formato de descriptores

- "hs-descriptor" SP version-number NL
- "descriptor-lifetime" SP LifetimeMinutes NL
- **"descriptor-signing-key-cert" NL certificate NL.**
- "revision-counter" SP Integer NL
- **"superencrypted" NL encrypted-string** # Cifrado con **credential**
- "signature" SP signature NL

- **subcredential** = H("subcredential" | **credential** | **blinded-public-key**)
- **credential** = H("credential" | **public-identity-key**)

Tor v3

Nuevo formato de descriptores

- En la versión 3 no vamos a poder sacar el dominio, porque se consulta una clave derivada mediante una técnica criptográfica conocida como *Blind signature*:

```
descriptor-lifetime 180
descriptor-signing-key-cert
-----BEGIN ED25519 CERT-----
AQgABnCHAX/lD22dsvl9tz+WjyflbJ7OX/+K1cEmRpER698vPNjsAQAgBABAimrQ
Gxj7tcge4aNy7XuMHgvf6JeMg8DOKhwN83BSOb9n4trSVHuybTwUVWPEF5b4KRaZ
vaBxe8Oe1krGkHzYtIR13jxqbXZdy1r0M2o8GbEYwKWUmRU58DzYIMx7vQQ=
-----END ED25519 CERT-----
...
```

Tor v3

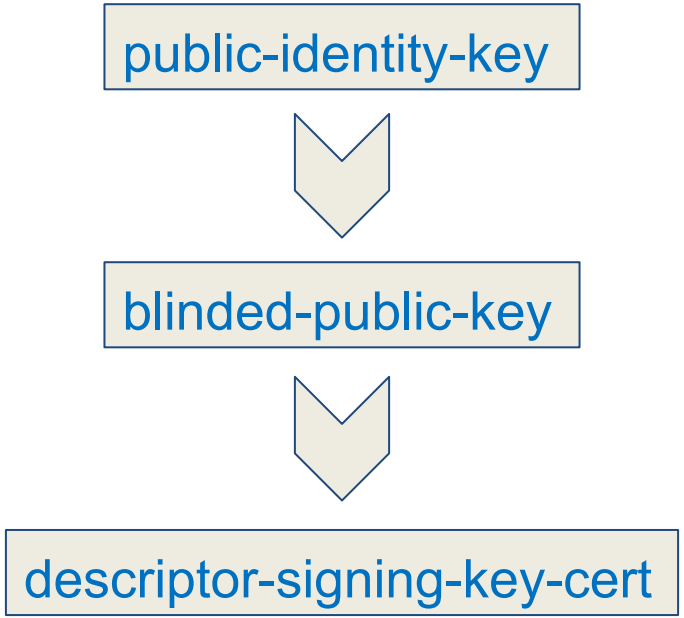
Nuevo formato de descriptores

- descriptor-signing-key-cert
  - Se firma con *blinded-public-key*
    - Que se deriva de *public-identity-key*
      - Que genera los dominios

- superencrypted
  - Se cifra con *subcredential*
    - Que se deriva de *credential*
      - Que se genera con *public-identity-key*
        - Que genera los dominios

Tor v3

Nuevo formato de descriptores



Tor v3

Principales diferencias

❖ Versión 3

- ➢ Van a seguir conviviendo las dos versiones
  - ■ La versión 3 todavía ha de sufrir modificaciones
- ➢ Para hacer usables los nuevos dominios (56 caracteres) se está planteando utilizar otros sistemas (estilo DNS o alias de dominio)
  - ■ Aumentará la usabilidad a costa de la seguridad

Conclusiones

¿Tiene sentido indexar todo?

- Muchos sitios delictivos necesitan darse a conocer
- Es más práctico escuchar las redes y conocer el entorno
- Obtención del flag Guard
  - Abre nuevas vías de investigación
  - Puede ser más interesante buscar cómo combatir los servicios que ya conocemos que esforzarse en conocer más

Trabajos futuros

Incorporación de nuevas redes y métodos de investigación

- Tor v3 supone un nuevo reto
  - Todavía en desarrollo y sujeto a cambios
  - Actualmente el uso de v3 es muy bajo
- Autenticación
  - Existen multitud de foros que requieren autenticación
  - Automatizar registro y autenticación
- Incorporar nuevas redes: Freenet
  - Al conectarnos a freenet compartimos archivos de la red
  - Multitud de contenido pedófilo en Freenet

Agradecimientos

Equipo de Investigación de la UAH

- Juan Ángel López Sanz

- Nicolas Logghe Barbini

Agradecimientos

Equipo de Investigación de la UAH

- Alvaro W. Schuller Fernández - David Moreno Moreno
- Enrique Larriba González

Agradecimientos

Equipo de Investigación de la UAH

- Dr. José Javier Martínez Herráiz

Universidad de Alcalá | Isdefe
Cátedra Ciberseguridad

Agradecimientos

Equipo de Investigación de la UAH

- Carlos Cilleruelo Rodríguez

ALPHA SECURITY

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectiva

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional