2. Técnicas DE INVESTIGACIÓN EN TOR PARTIENDO DE FUENTES ABIERTAS

Las mismas técnicas vistas en el tema anterior pueden ser extrapoladas a la investigación de amenazas dentro de Tor, tan solo variarán las fuentes que consultemos y la forma de acceso a este tipo de Darknet. Por este hecho, en la presente sección veremos una serie de fuentes que podremos utilizar dentro de la Surface Web para localizar dominios .onion y luego posteriormente consultar otras fuentes más ocultas dentro de la propia red Tor.

2.1. BUSCADORES DE HIDDEN SERVICES DE TOR EN FUENTES ABIERTAS

En este apartado se pueden encontrar una serie de buscadores que van a permitir localizar enlaces de dominios .onion, realizando consultas desde la Surface Web utilizando palabras clave concretas.

2.1.1. DANIEL HOSTING

Daniel Hosting era uno de los ISP más conocidos sobre Hidden Services en Internet, pero debido a un ataque en 2020 donde filtraron toda la BBDD en Internet, Daniel Winzen (creador de Daniel Hosting) decidió no continuar como proveedor de alojamiento de dominios .onion (ver Imagen 95). Se dispone de más información en el siguiente enlace: https://www.infobae.com/america/tecno/2020/06/03/se-filtro-la-base-de-datos-de-uno-de-los-servicios-de-hosting-mas-grandes-de-la-dark-web/.

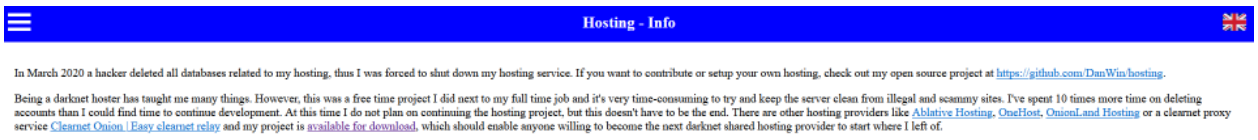


Imagen 95. Sitio web de Daniel Hosting indicando que ya no ofrece servicios de hosting en Tor

Daniel Hosting permite el acceso a su sitio web por dos vías:

- Surface Web: https://danwin1210.de.
- Tor: http://danielas3rtn54uwmofdo3x2bsdifr47huasnmbgqzfrec5ubupvtpid.onion/

Daniel Hosting ofrece los siguientes recursos dentro de su sitio web:

- Un verificador de si un Hidden Service de Tor está activo o no. En la Imagen 96 se puede ver una prueba con el dominio .onion de Daniel Hosting. El acceso está disponible en el siguiente enlace: https://onions.danwin1210.de/test.php.

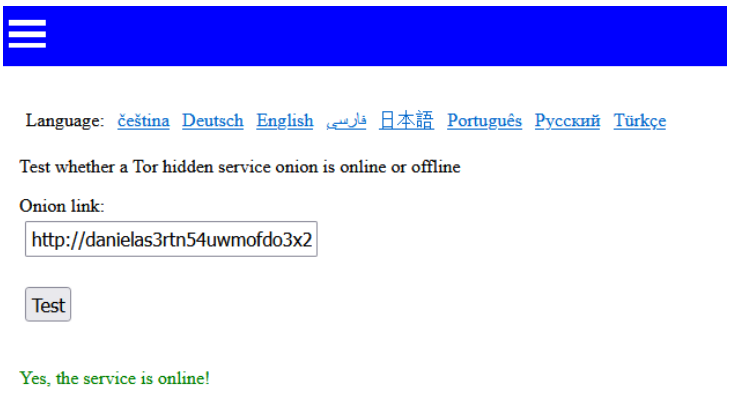


Imagen 96. Verificador de dominios .onion con Daniel Hosting

- Un buscador para realizar diferentes consultas para localizar dominios de Tor. En la Imagen 97 se puede ver lo comentado. El acceso está disponible en el siguiente enlace: https://onions.danwin1210.de/.

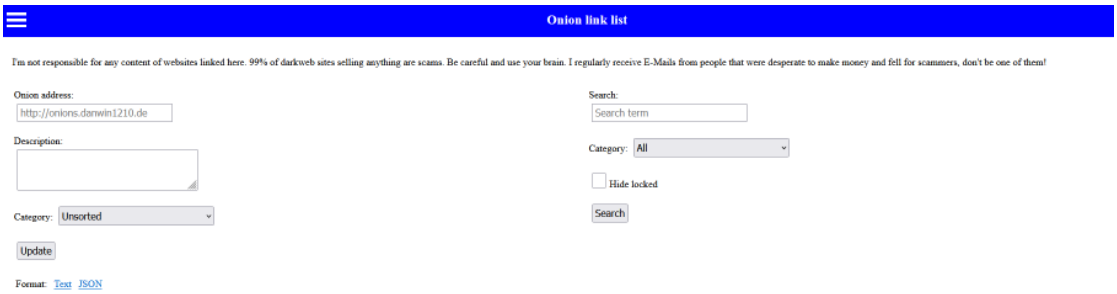


Imagen 97. Buscador de dominio .onion de Daniel Hosting

Ahora, procedemos a realizar una consulta de la palabra clave "ransomware" dentro del buscador, el cual nos devuelve un único resultado relacionado con un dominio .onion en el que su descripción hace mención a un sitio web relacionado con sitios de grupos de ransomware. Lo mencionado puede verse en la Imagen 98.

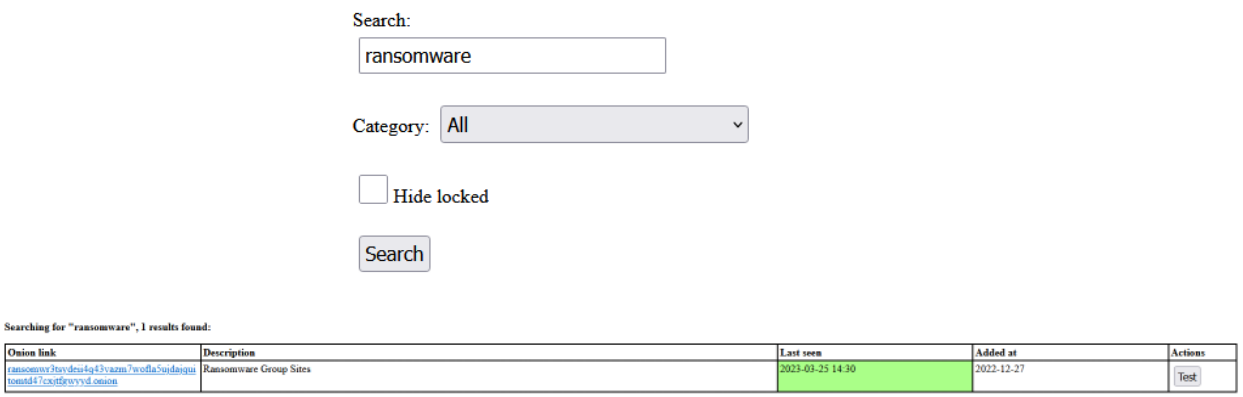
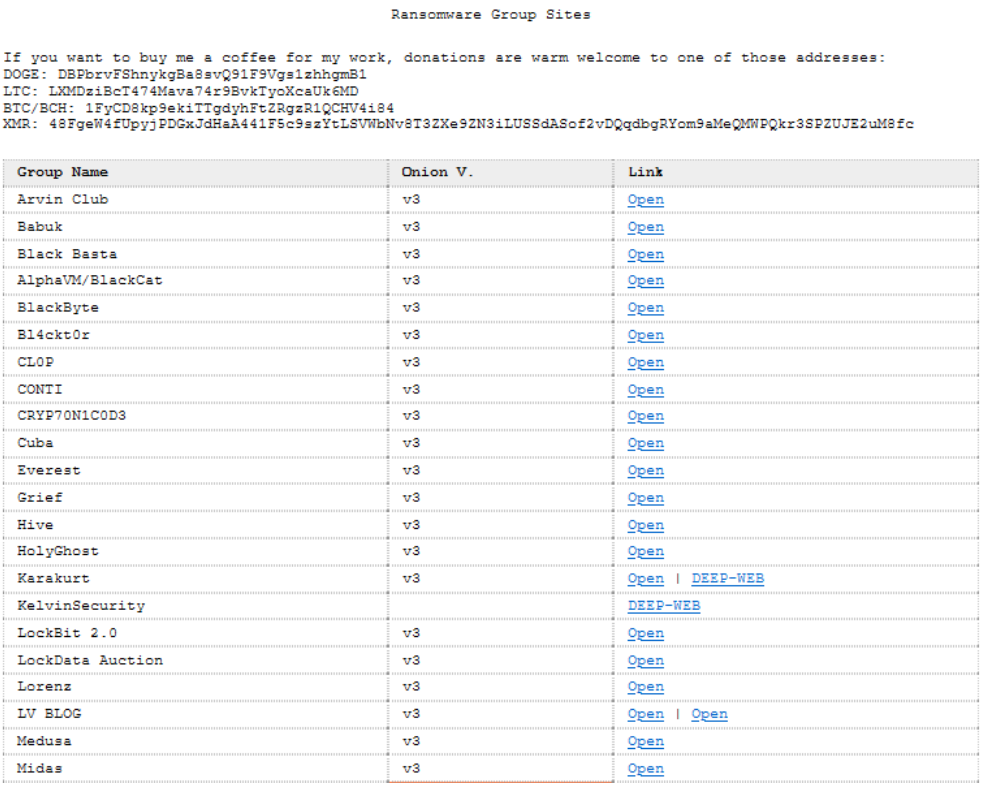


Imagen 98. Búsqueda de la palabra clave "ransomware" dentro de Daniel Hosting

Si ahora abrimos nuestro Tor Browser y accedemos al dominio .onion recolectado, podremos ver su contenido relacionado y valoraremos si el mismo puede llegar a ser interesante como fuente o no. Dicho contenido puede verse en la Imagen 99, siendo un inventario de grupos de ransomware con su respectivo enlace .onion.



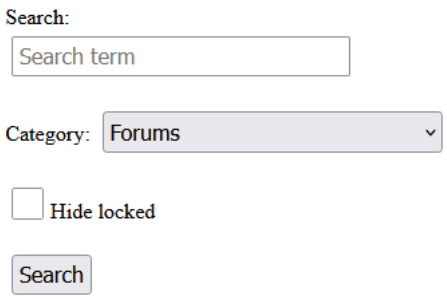
Ransomware Group Sites

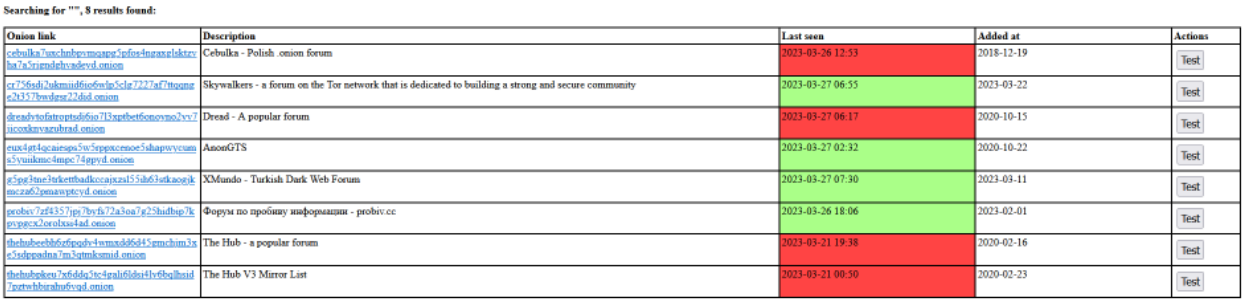
If you want to buy me a coffee for my work, donations are warm welcome to one of those addresses:
DOGE: DBPbrvFShnykgBa8svQ91F9Vgs1zhhgmB1
LTC: LXMDziBcT474Mava74r9BvkTyoXcaUk6MD
BTC/BCH: 1FyCD8kp9ekiTTgdyhFtZRgzR1QCHV4i84
XMR: 48FgeW4fUpyjPDGxJdHaA441F5c9szYtLSVWbNv8T3ZXe9ZN3iLUSSdASof2vDQqdbgRYom9aMeQMWPQkr3SPZUJE2uM8fc

Group Name	Onion V.	Link
Arvin Club	v3	Open
Babuk	v3	Open
Black Basta	v3	Open
AlphaVM/BlackCat	v3	Open
BlackByte	v3	Open
Bl4ckt0r	v3	Open
CL0P	v3	Open
CONTI	v3	Open
CRYP70N1C0D3	v3	Open
Cuba	v3	Open
Everest	v3	Open
Grief	v3	Open
Hive	v3	Open
HolyGhost	v3	Open
Karakurt	v3	Open | DEEP-WEB
KelvinSecurity		DEEP-WEB
LockBit 2.0	v3	Open
LockData Auction	v3	Open
Lorenz	v3	Open
LV BLOG	v3	Open | Open
Medusa	v3	Open
Midas	v3	Open

Imagen 99. Enlace del dominio .onion recolectado mediante Daniel Hosting

Ahora realizaremos otra consulta filtrando por la categoría de foros y sin utilizar ninguna palabra clave. En la Imagen 100 pueden verse los enlaces .onion recolectados, indicando cuales están operativos o inoperativos.





Searching for "", 8 results found:

Onion link	Description	Last seen	Added at	Actions
cebulka7uxchnbpvmqapg5pfos4ngaxglsktzzbu7a5rignqdhyadeyd.onion	Cebulka - Polish .onion forum	2023-03-26 12:53	2018-12-19	Test
cr756sdi2ukmiid6io6wlp5cla7227af7ttoqnqe2t357bwdgsr22did.onion	Skywalkers - a forum on the Tor network that is dedicated to building a strong and secure community	2023-03-27 06:55	2023-03-22	Test
dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion	Dread - A popular forum	2023-03-27 06:17	2020-10-15	Test
eux4gt4qcairsqs5w5eppxcenoe5shapwycumc5yunknc4mpc74qpyd.onion	AnonGTS	2023-03-27 02:32	2020-10-22	Test
g5pg3tne3trkettbadkccajxzsl55ih63stkaogjkmcza62pmawptcyd.onion	XMundo - Turkish Dark Web Forum	2023-03-27 07:30	2023-03-11	Test
probsv7zf4357jpi7bvfk72a3oa7g25hidbsp7kpvpqcx2orolxss4ad.onion	Форум по пробиву информации - probiv.cc	2023-03-26 18:06	2023-02-01	Test
thehubeebbfzfpqdv4wmxdd6d45gmchjm3se5sdppadna7m3qtmksmid.onion	The Hub - a popular forum	2023-03-21 19:38	2020-02-16	Test
thehubpkeu7x6ddq5tc4grali6ldsj4ly6bqlhsid7pttvhbsrahu6vqd.onion	The Hub V3 Mirror List	2023-03-21 00:50	2020-02-23	Test

Imagen 100. Resultados de dominios .onion relacionados con foros

2.1.2. AHMIA

AHMIA es un buscador accesible desde la Surface Web, el cual, permite realizar consultas mediante palabras clave para detectar dominios .onion. AHMIA utiliza una serie de crawlers que van detectando nuevos dominios .onion, almacenándolas dentro de su base de datos.

AHMIA permite el acceso a su sitio web por dos vías:

- Surface Web: https://ahmia.fi/.
- Tor: http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/

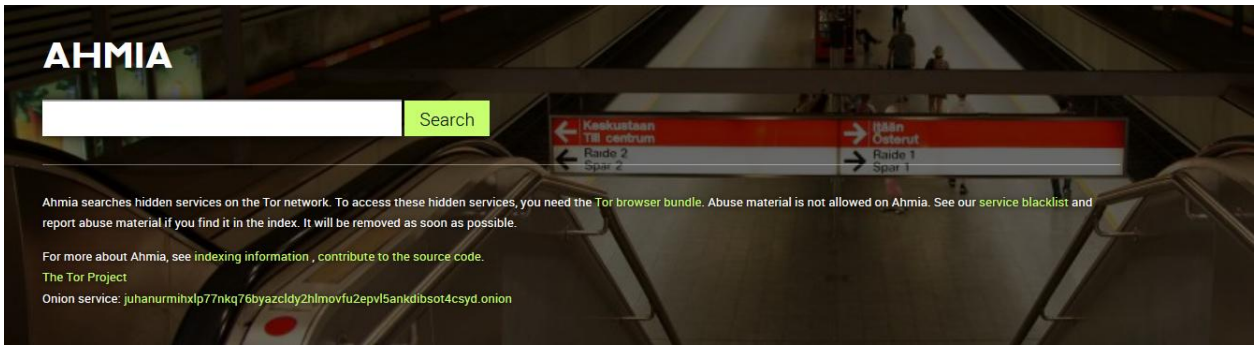


Imagen 101. Sitio web oficial de AMHIA

AHMIA ofrece los siguientes recursos dentro de su sitio web:

- Permite visualizar estadísticas tanto de manera visual mediante grafos (Imagen 103) o por gráfica de barras (Imagen 104). El acceso está disponible en el siguiente enlace: https://ahmia.fi/stats/.

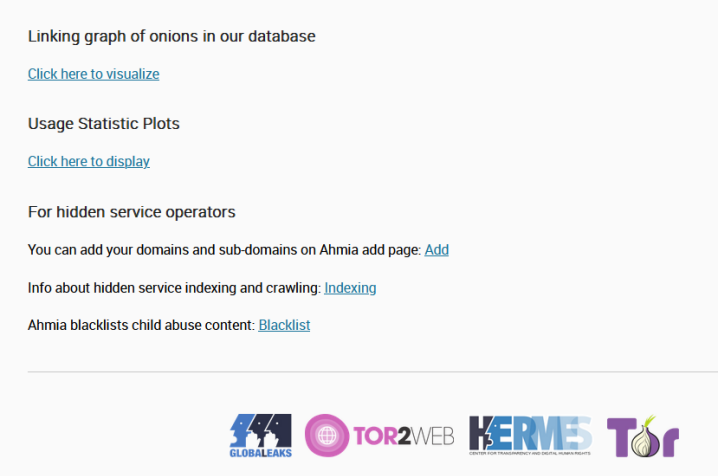


Imagen 102. Diferentes opciones de visualización de estadísticas sobre dominios .onion

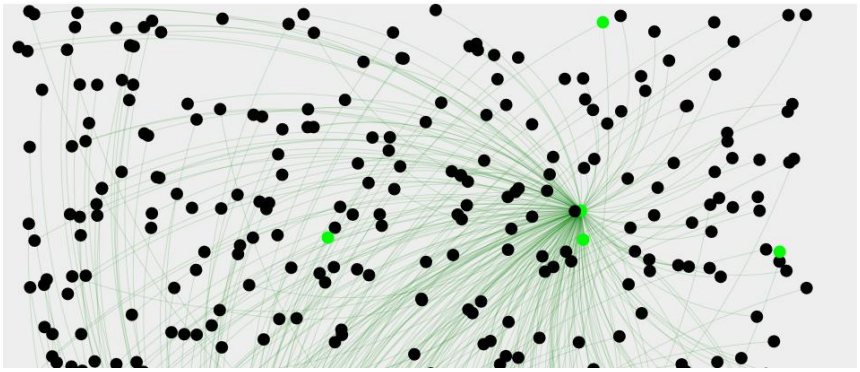


Imagen 103. Estadísticas de dominios .onion representados mediante grafos

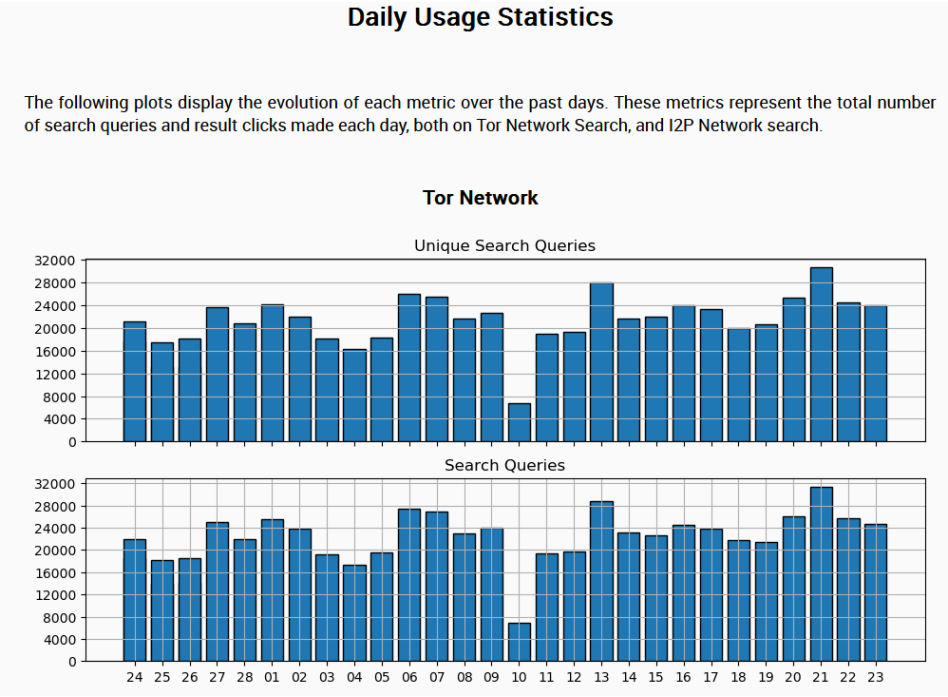


Imagen 104. Estadísticas de uso diario de dominio .onion

- Permite consultar un listado de dominios .onion que AHMIA tiene indexados en su base de datos interna. El acceso está disponible directamente en el siguiente enlace: https://ahmia.fi/onions/. En la Imagen 105 puede verse un extracto del listado.

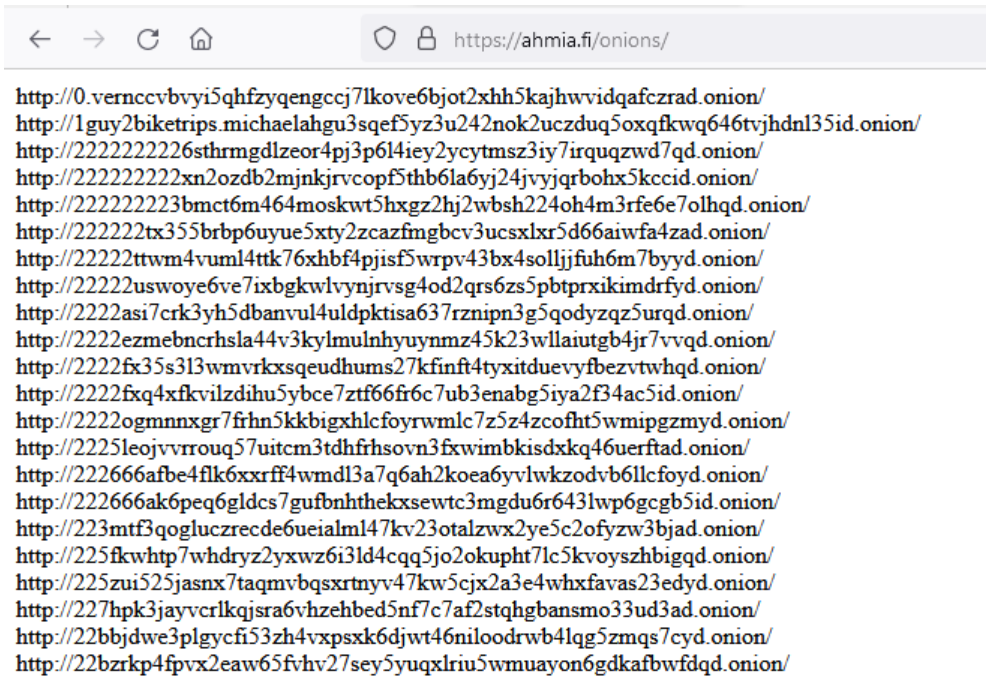


Imagen 105. Listado de dominios .onion indexados por AHMIA

- Un buscador para realizar diferentes consultas para localizar dominios .onion. En la Imagen 106 se puede ver lo comentado. El acceso está disponible directamente desde el sitio web principal: https://ahmia.fi/.

Ahora, procedemos a realizar la consulta de la palabra clave "ransomware" dentro de AHMIA, el cual nos devuelve 236 resultados relacionados con dominios .onion. Lo mencionado puede verse en la Imagen 106.

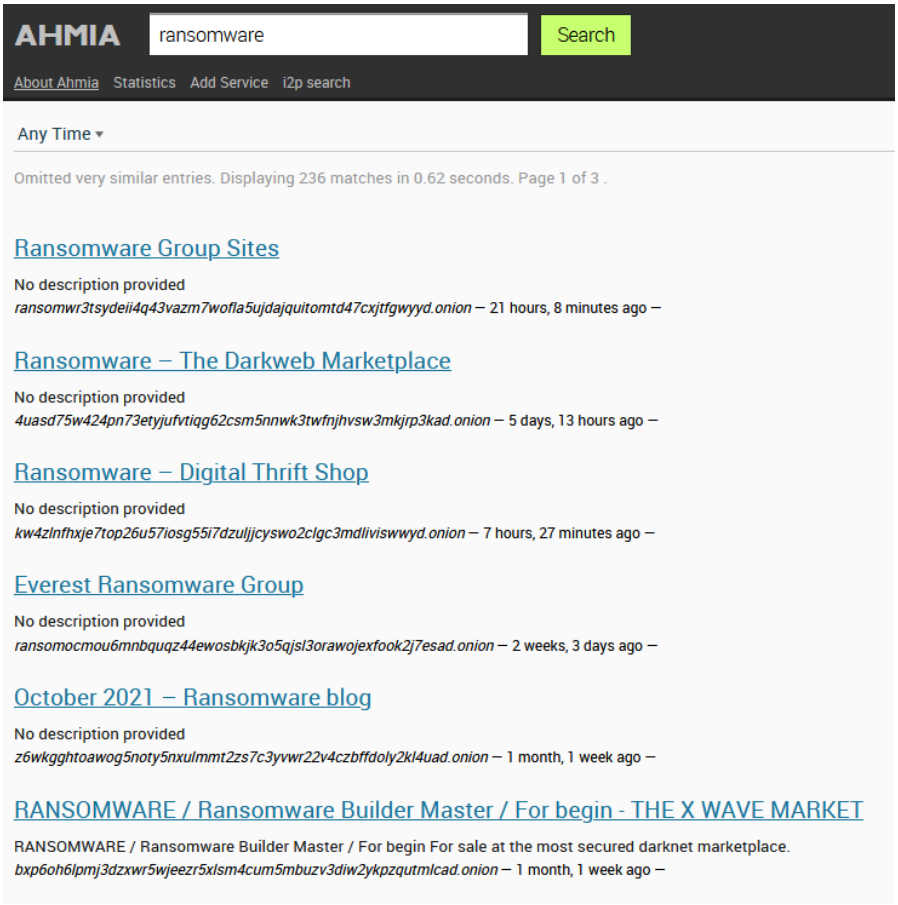


Imagen 106. Resultado de la palabra clave "ransomware" en AHMIA

2.1.3. ONIONLAND

OnionLand es un buscador accesible desde la Surface Web, el cual, tal como ocurre con AHMIA permite realizar consultas mediante palabras clave para detectar dominios .onion. OnionLand utiliza una serie de crawlers que van detectando nuevos dominios .onion, almacenándolas dentro de su base de datos.

OnionLand permite el acceso a su sitio web por dos vías:

- Surface Web: https://onionlandsearchengine.com/.
- Tor: http://3bbad7fauom4d6sgppalyqddsqbf5u5p56b5k5uk2zxsy3d6ey2jobad.onion/

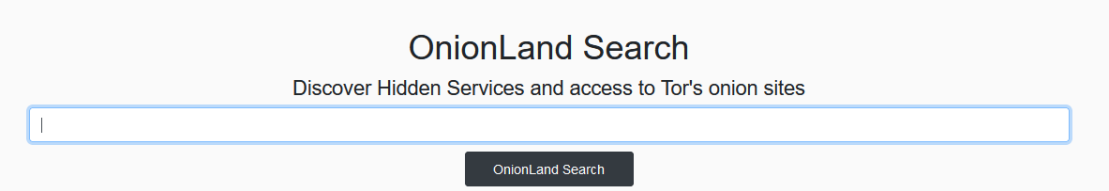


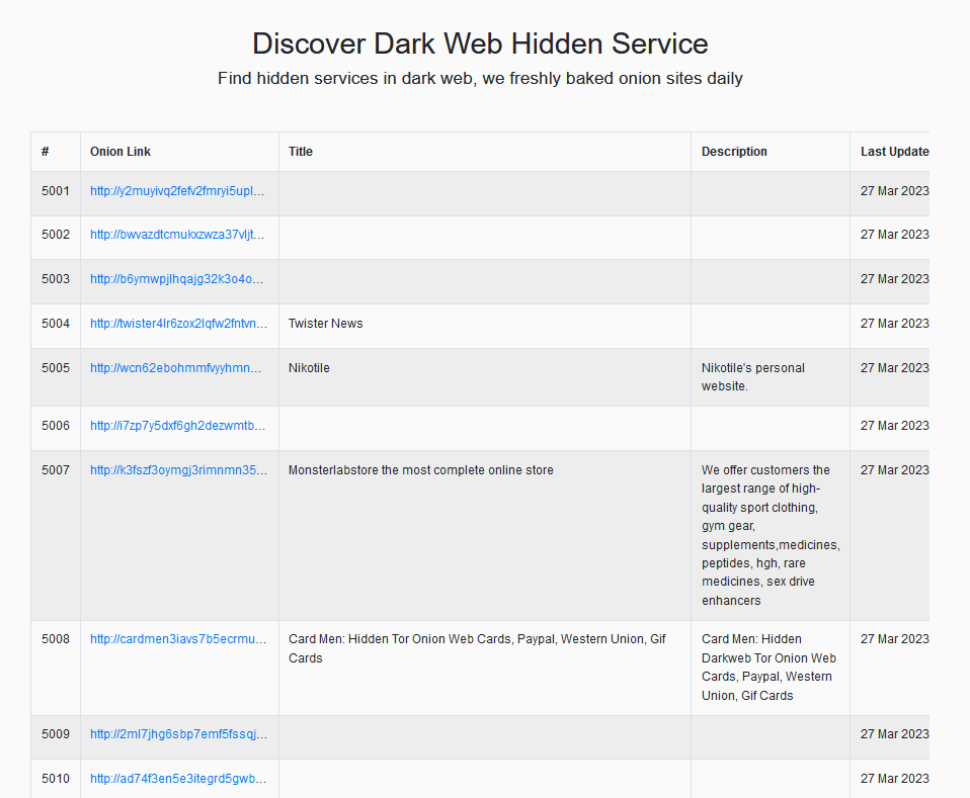
Imagen 107. Sitio Oficial de OnionLand

OnionLand ofrece los siguientes recursos dentro de su sitio web:

- Dispone de un inventario de los últimos dominios .onion junto con una descripción, título de la web (en algunos casos) y fecha de actualización. En la Imagen 108 puede verse un ejemplo de lo mencionado. El acceso está disponible en el siguiente enlace: https://onionlandsearchengine.com/discover.

- Dispone de un inventario de términos de búsqueda más demandados, ordenados alfabéticamente. En la Imagen 109 puede verse un ejemplo de lo mencionado. El acceso está disponible en el siguiente enlace: https://onionlandsearchengine.com/most-popular.

Con este buscador hay que tener bastante cuidado (tal como se puede llegar a comprobar en la Imagen 109) porque no realiza ningún tipo de filtrado con los términos de búsqueda detectados e indexados, lo que implica que podamos encontrarnos con enlaces hacia contenido muy delicado como el abuso y explotación infantil.

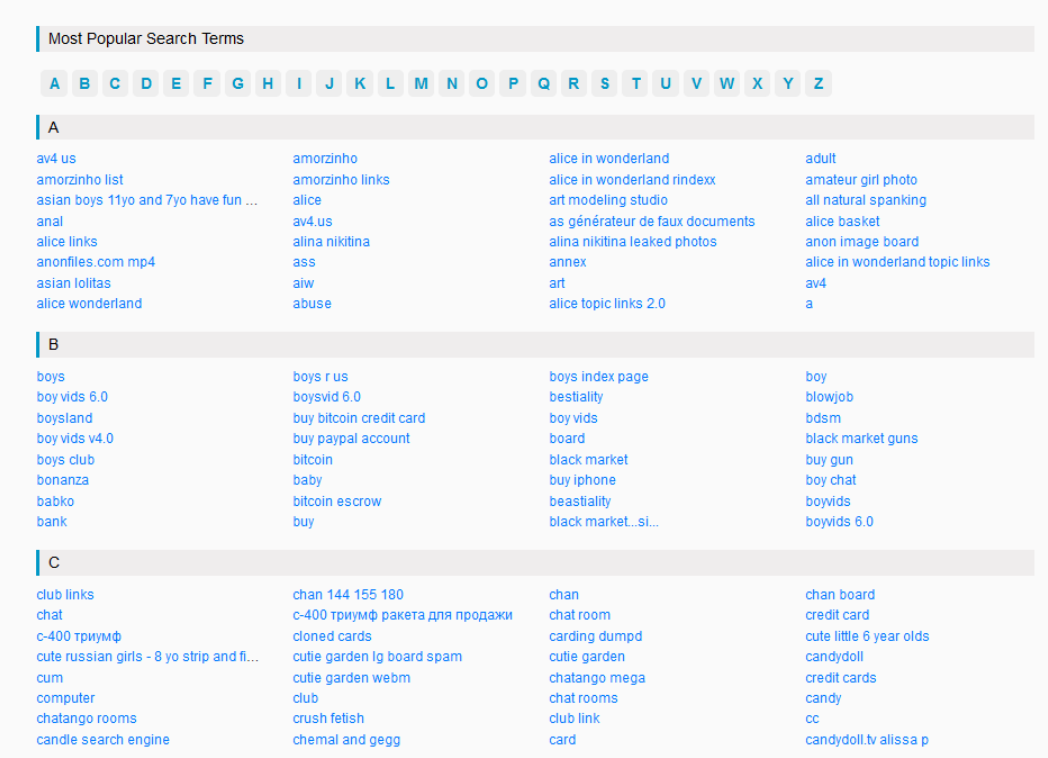


Discover Dark Web Hidden Service

Find hidden services in dark web, we freshly baked onion sites daily

#	Onion Link	Title	Description	Last Update
5001	http://y2muyivq2fefv2fmryi5upl...			27 Mar 2023
5002	http://bwvazdtcmukxzwza37vljt...			27 Mar 2023
5003	http://b6ymwpjlhqajg32k3o4o...			27 Mar 2023
5004	http://twister4lr6zox2lqfw2fntvn...	Twister News		27 Mar 2023
5005	http://wcn62ebohmmfvyyhmn...	Nikotile	Nikotile's personal website.	27 Mar 2023
5006	http://i7zp7y5dxf6gh2dezwmtb...			27 Mar 2023
5007	http://k3fszf3oymgj3rimnmn35...	Monsterlabstore the most complete online store	We offer customers the largest range of high-quality sport clothing, gym gear, supplements,medicines, peptides, hgh, rare medicines, sex drive enhancers	27 Mar 2023
5008	http://cardmen3iavs7b5ecrmu...	Card Men: Hidden Tor Onion Web Cards, Paypal, Western Union, Gif Cards	Card Men: Hidden Darkweb Tor Onion Web Cards, Paypal, Western Union, Gif Cards	27 Mar 2023
5009	http://2mi7jhg6sbp7emf5fssqj...			27 Mar 2023
5010	http://ad74f3en5e3itegrd5gwb...			27 Mar 2023

Imagen 108. Discover de Hidden Services de OnionLand



Most Popular Search Terms

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

av4 us	amorzinho	alice in wonderland	adult
amorzinho list	amorzinho links	alice in wonderland rindexx	amateur girl photo
asian boys 11yo and 7yo have fun ...	alice	art modeling studio	all natural spanking
anal	av4.us	as générateur de faux documents	alice basket
alice links	alina nikitina	alina nikitina leaked photos	anon image board
anonfiles.com mp4	ass	annex	alice in wonderland topic links
asian lolitas	aiw	art	av4
alice wonderland	abuse	alice topic links 2.0	a

B

boys	boys r us	boys index page	boy
boy vids 6.0	boysvid 6.0	bestiality	blowjob
boysland	buy bitcoin credit card	boy vids	bdsm
boy vids v4.0	buy paypal account	board	black market guns
boys club	bitcoin	black market	buy gun
bonanza	baby	buy iphone	boy chat
babko	bitcoin escrow	beastiality	boyvids
bank	buy	black market...si...	boyvids 6.0

C

club links	chan 144 155 180	chan	chan board
chat	c-400 триумф ракета для продажи	chat room	credit card
c-400 триумф	cloned cards	carding dumpd	cute little 6 year olds
cute russian girls - 8 yo strip and fi...	cutie garden lg board spam	cutie garden	candydoll
cum	cutie garden webm	chatango mega	credit cards
computer	club	chat rooms	candy
chatango rooms	crush fetish	club link	cc
candle search engine	chemal and gegg	card	candydoll.tv alissa p

Imagen 109. Términos más buscados en OnionLand ordenados alfabéticamente

2.1.4. DARKFEED

DarkFeed es un servicio online que ofrece información sobre incidentes de ransomware, permitiendo realizar un seguimiento de estos en cuanto a volumetría. Recientemente, DarkFeed ha creado diferentes tipos de suscripciones, una gratuita y dos de pago. El acceso está disponible en el siguiente enlace: https://darkfeed.io.

En la Imagen 110 se puede ver el sitio web oficial de DarkFeed, el cual recoge información sobre los últimos ataques por ransomware, el top 8 de los grupos asociados que están activos en la actualidad, top 10 del total de grupos según la victimología y el top 10 de ataques dirigidos hacia países concretos.

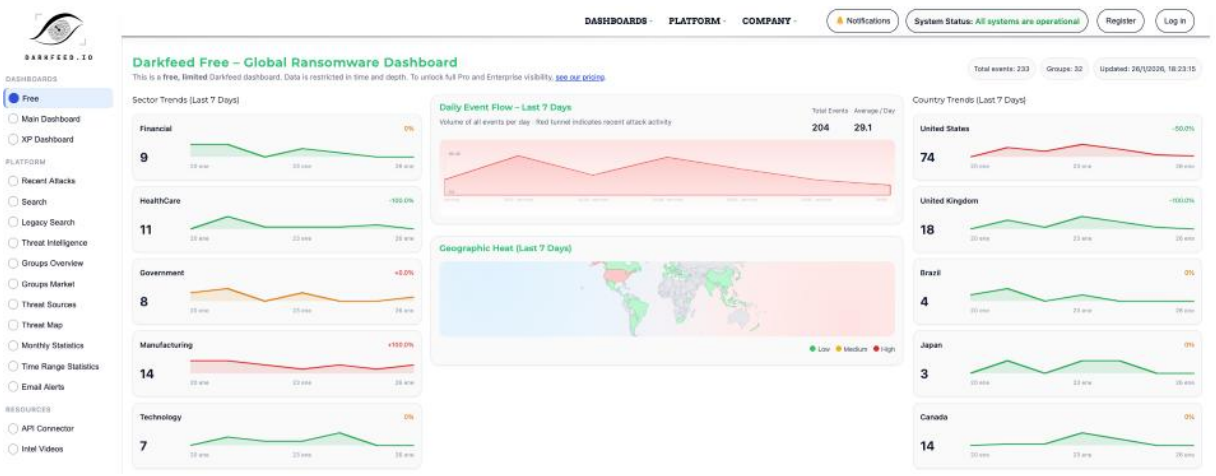


Imagen 110. Volumetrías sobre incidentes de ransomware ofrecidos por DarkFeed

DarkFeed ofrece también de manera gratuita un inventario con información relacionada con los grupos de ransomware, donde se puede ver un listado con los grupos que están activos, el total de víctimas de cada grupo, la última víctima, lugar de alojamiento del sitio web oficial de cada grupo (Tor, Surface Web o Telegram) y estado del grupo (activo o inactivo). En la Imagen 111 puede visualizarse lo comentado. El acceso al recurso está disponible en el siguiente enlace: https://darkfeed.io/groups-overview/.

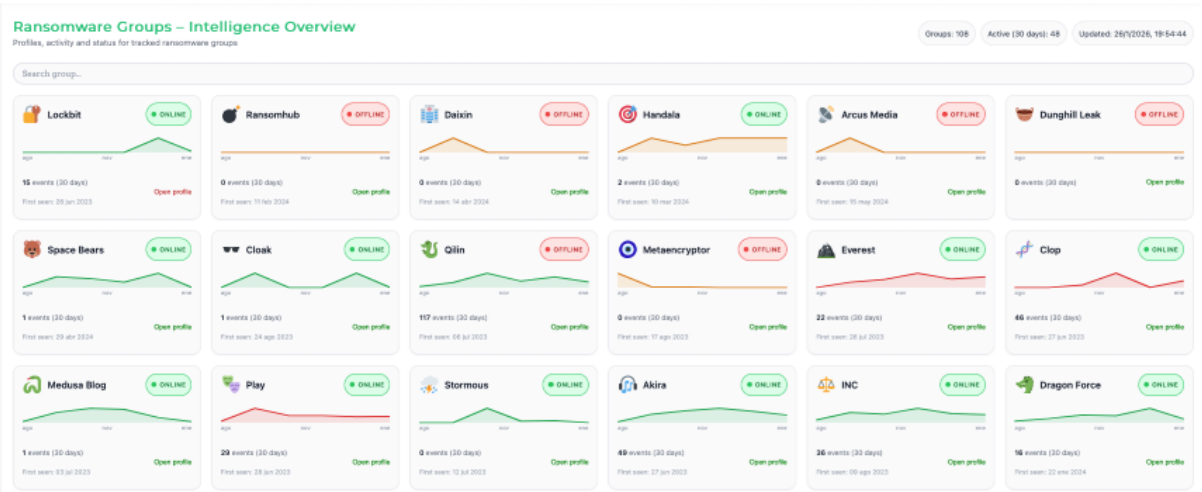


Imagen 111. Listado de grupos de ransomware en DarkFeed

2.1.5. STEALTHmole

StealthMole es un servicio online de pago que está formado por un conjunto de módulos que ofrece información de diversa índole, tales como fugas de información, monitorización de ataques de ransomware, credenciales expuestas, tracking de transacciones con criptomonedas, análisis de dominios de la Dark Web, etc. El acceso está disponible en el siguiente enlace: https://www.stealthmole.com/.

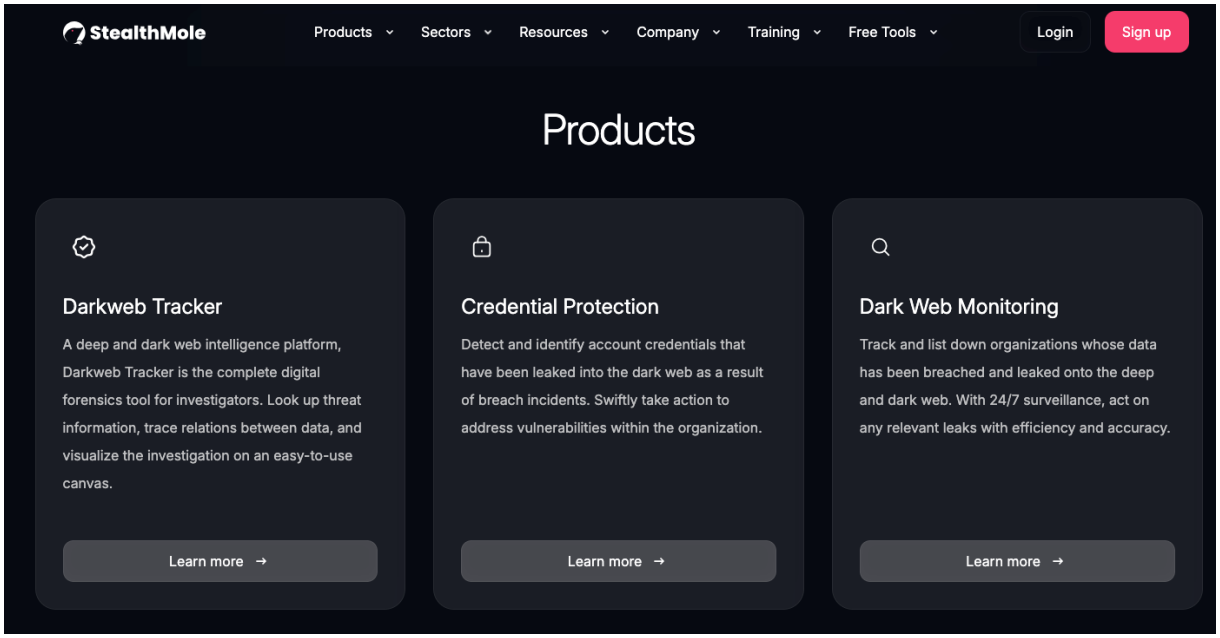


Imagen 112. Servicios ofrecidos por StealthMole

En la actualidad dispone de un total de 214 billones de datos almacenados en sus propias bases de datos internas, 1,2 millones de direcciones .onions, monitorización de 58.889 dominios .onion en tiempo real y un total de 5.989 direcciones IP. En la Imagen 113 puede comprobarse lo mencionado.

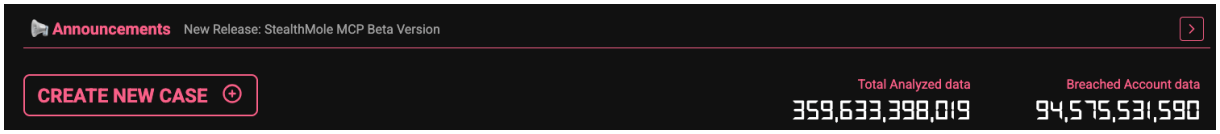


Imagen 113. Volumetría de contenido de datos de StealthMole

StealthMole permite crear una cuenta gratuita por medio de un correo corporativo, donde se dispone de un módulo totalmente gratuito de monitorización de víctimas de ransomware, ofreciendo un pequeño inventario sobre cada ataque. Para ello es necesario

acceder al "Extension Packs" para seleccionar y añadir el módulo de "Ransomware Monitoring" tal como se puede ver en la Imagen 114.

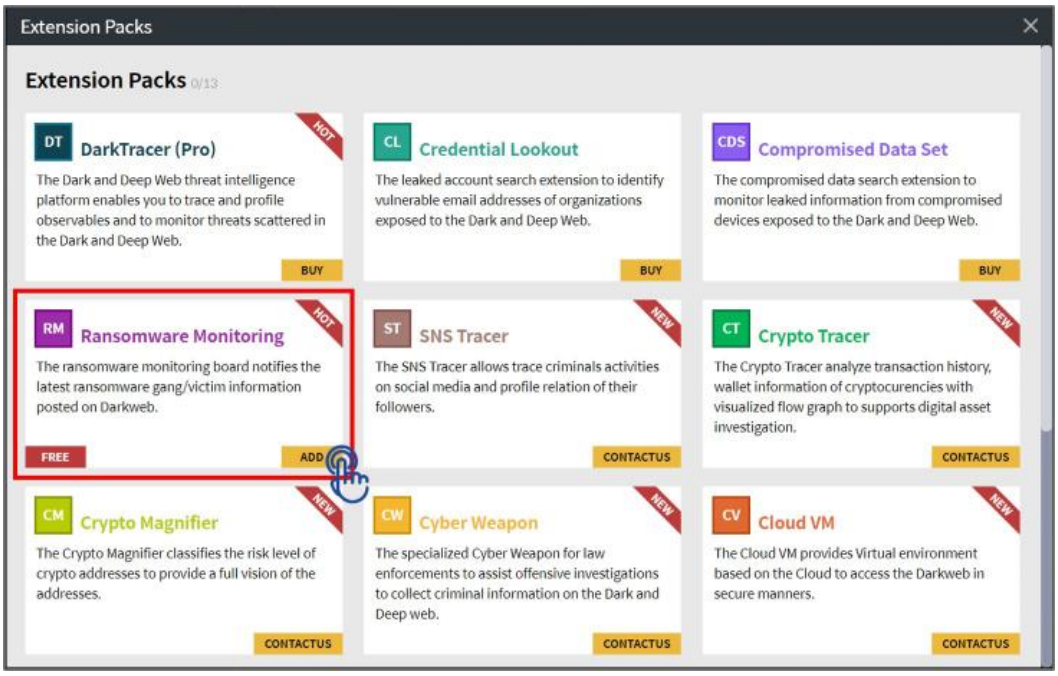


Imagen 114. Añadir modulo gratuito de StealthMole sobre ransomware

En el momento que tengamos añadido dicho módulo se podrá acceder al portal Ransomware Monitoring (RM) para realizar un seguimiento e investigar víctimas de ransomware. En la Imagen 115 puede verse lo mencionado, donde se puede recolectar información de cada ataque de ransomware conocido de manera pública (por medio de las difusiones de los distintos grupos de ransomware en su correspondiente sitio web) como por ejemplo el nombre de la víctima, su sitio web, país de origen, sector, la fecha de detección, junto con el grupo de ransomware relacionado. Además, es posible representar cada tipo de dato en un grafo con relaciones. StealthMole nos permite realizar un total de 30 peticiones de manera gratuita al mes, por lo que se deberá tener cuidado de no abusar de ellas con facilidad.

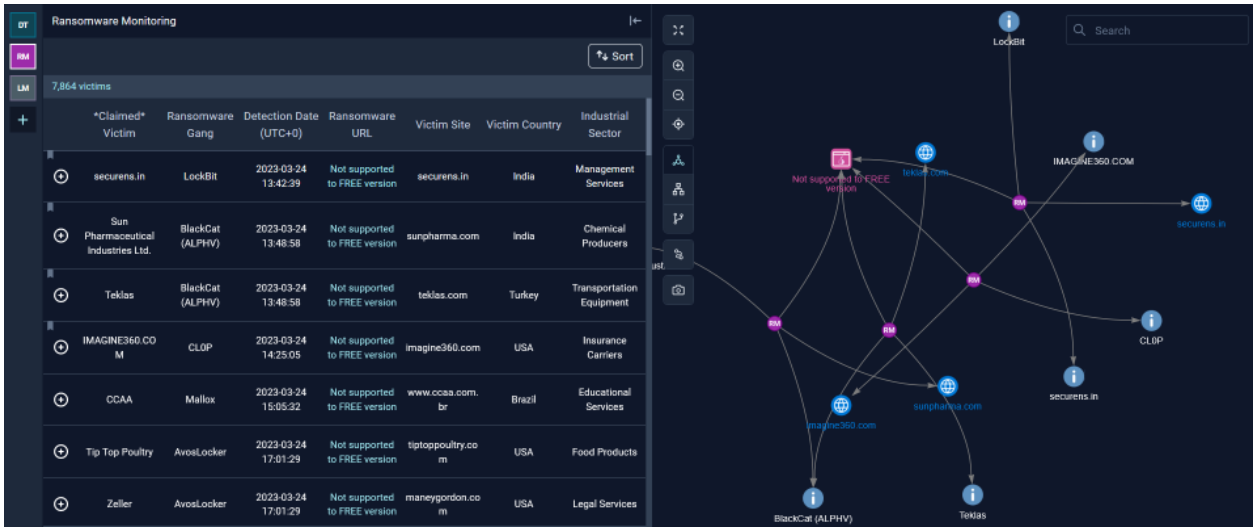


Imagen 115. Portal del módulo de Ransomware Monitoring de StealthMole

Por otro lado, StealthMole permite realizar un total de 100 consultas gratuitas al mes dentro de su módulo StealthMole (DT), para realizar cualquier tipo de investigación, pero con ciertas limitaciones al tener la cuenta gratuita.

Ahora, procedemos a realizar una consulta de la palabra clave “ransomware” dentro de StealthMole, el cual representa dicha palabra clave dentro del grafo y devuelve una serie de dominios y URLs de Tor y de I2P (visible en la cuenta gratuita) y otros tipos de datos (no visibles con la cuenta gratuita). Lo mencionado puede verse en la Imagen 116.

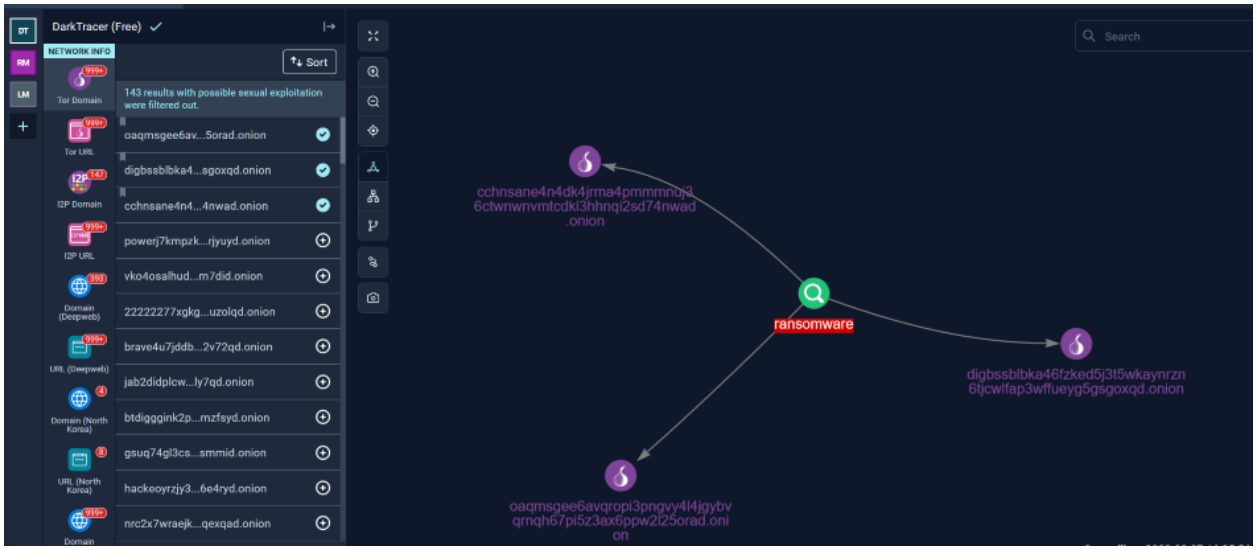


Imagen 116. Búsqueda de la palabra clave "ransomware" en StealthMole

Todos los enlaces que se detecten pueden ser añadidos en el grafo para su investigación. Si se intenta obtener más detalle de cada nodo del grafo, se comprobará que no nos lo permitirá ya que se necesitará una cuenta de pago, tal como se puede apreciar en la Imagen 117.

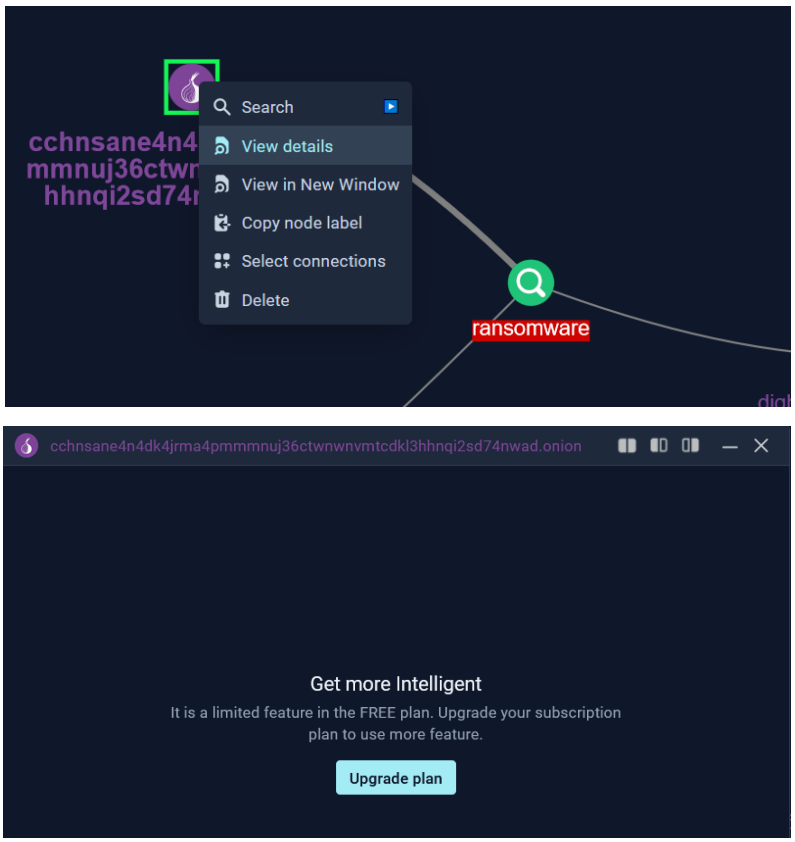


Imagen 117. Intento de ver detalle de un dominio añadido al grafo

En el caso de las URLs que se detectan de Tor, la herramienta sí que permite acceder al detalle de su contenido de manera gratuita, tal como se puede ver en la Imagen 118. Entre los datos que se detectan de la URL, se puede encontrar un screenshot del sitio web, la URL, fecha de escaneo, tamaño del contenido, hash, visualización del texto del sitio web y de su código fuente.

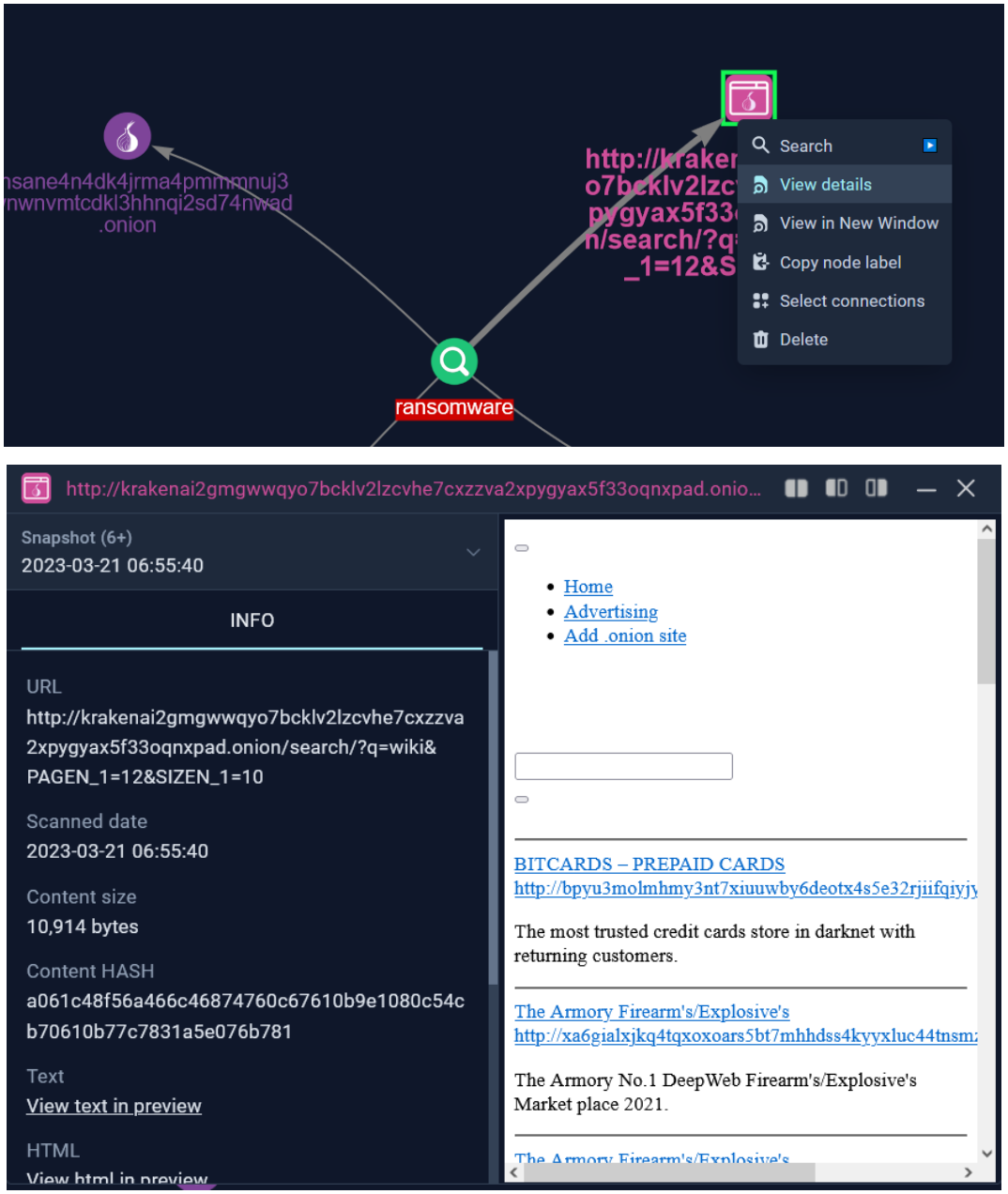


Imagen 118. Contenido de una URL de un dominio de Tor ofrecida pro StealthMole

En el caso de los dominios y URLs de I2P ocurriría exactamente lo mismo que se ha visto con los dominios de Tor.

2.2. BUSCADORES DE HIDDEN SERVICES DENTRO DE TOR

Hasta ahora hemos visto diferentes técnicas empleadas dentro de la Surface Web como punto de partida y saltar a la red Tor en un segundo paso. En este caso se va a acceder directamente a la red Tor, saliendo de lo que son las fuentes abiertas, pero es interesante conocer ciertas fuentes para consultar Hidden Services concretos a lo largo de una investigación.

2.2.1. THE HIDDEN WIKI

The Hidden Wiki es un servicio muy similar a la Wikipedia pero en este caso centrado en la red Tor, permitiendo el acceso a diferentes dominios .onion categorizados por tipos. El acceso al enlace es el siguiente: http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

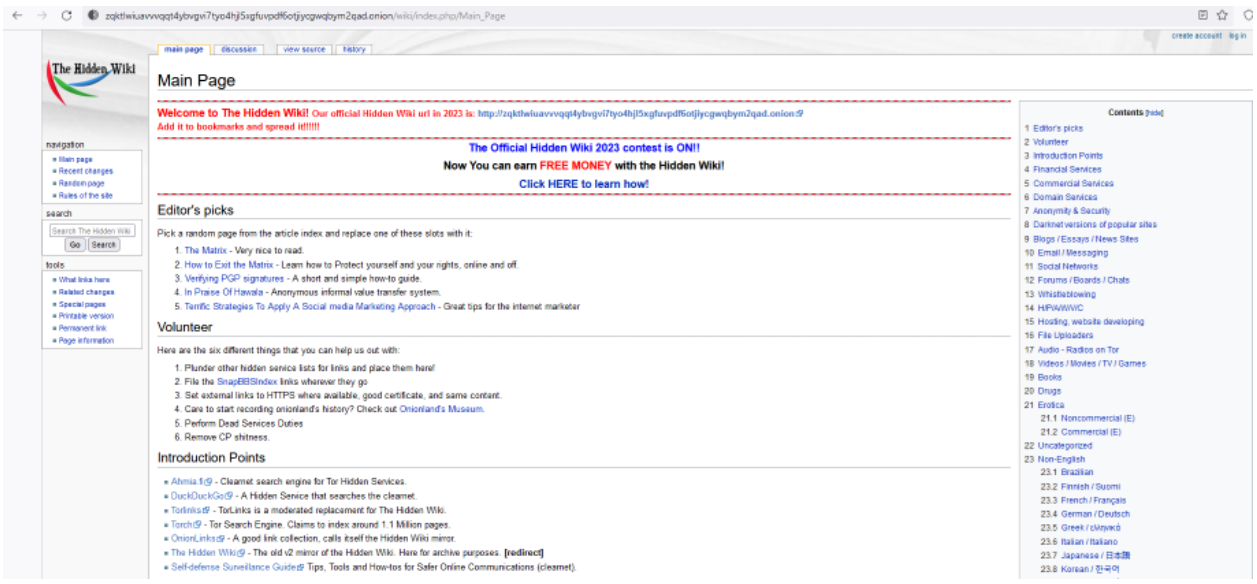


Imagen 119. Sitio web principal de The Hidden Wiki

2.2.2. TORCH

TORCH es un buscador que permite realizar consultas dentro de la red Tor para descubrir contenido en dicha Darknet. En la actualidad tiene indexado un total de 1,7 millones de documentos, tal como se puede observar en la Imagen 120.

El acceso al enlace es el siguiente: http://xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion.

Imagen 120. Sitio web de TORCH

Ahora, procedemos a realizar una consulta de la palabra clave "ransomware" dentro del buscador, el cual nos devuelve *3.235 resultados*. En la Imagen 121 se puede observar que obtenemos el título y una breve descripción de cada enlace .onion, junto con la URL y la palabra clave coincidente en la búsqueda.

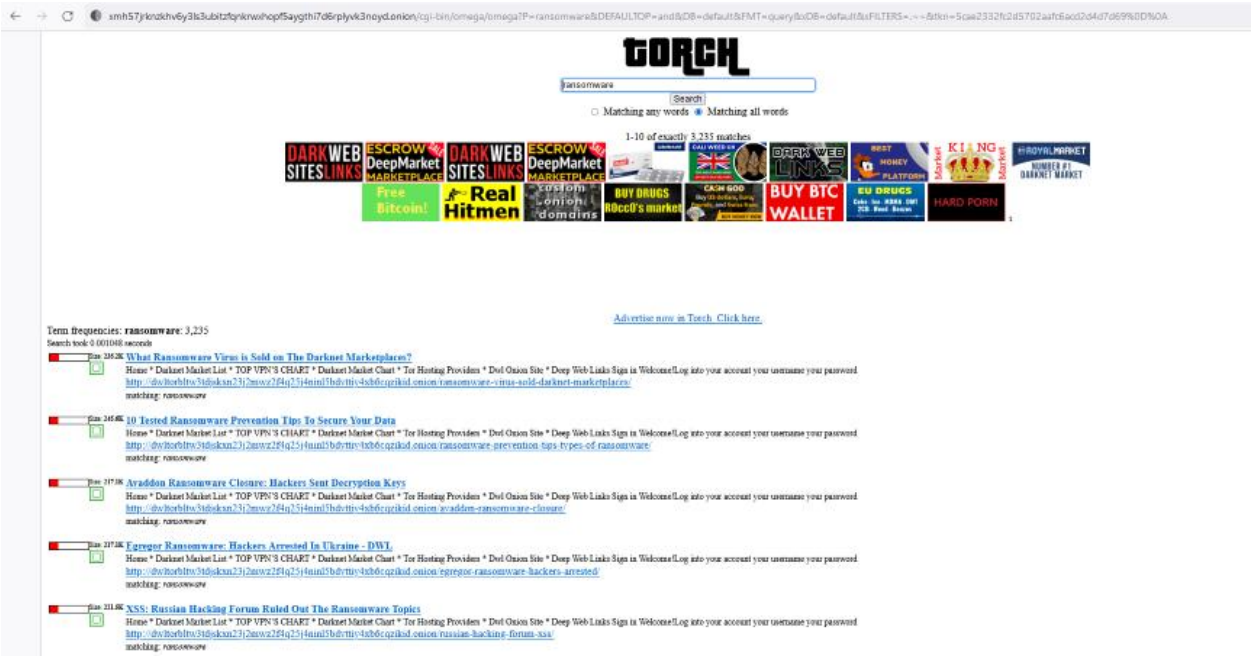


Imagen 121. Resultados de la palabra clave "ransomware" en TORCH

Si se accede al quinto enlace de la Imagen 121 se puede acceder al propio contenido de la URL .onion detectada, siendo un repositorio a modo inventario sobre black markets, foros relacionados con el cibercrimen, etc. En la Imagen 122 puede verse lo mencionado. Además, navegando por el sitio web se puede descubrir una sección sobre canales de Telegram relacionado con la misma temática anterior (ver Imagen 123)

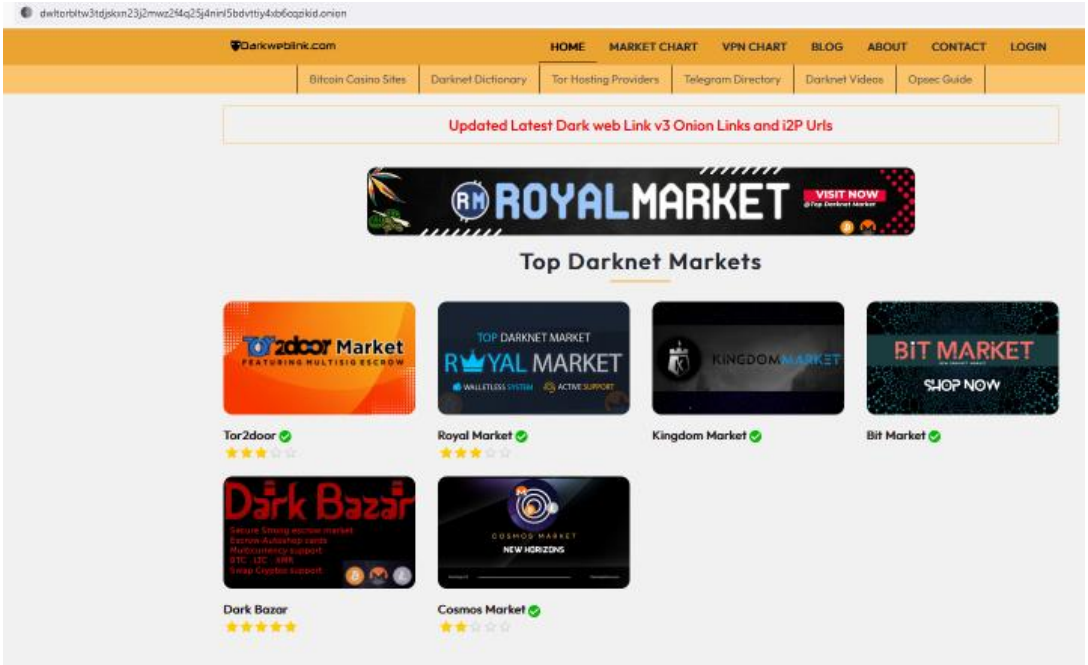


Imagen 122. Sitio web en Tor descubierto con TORCH

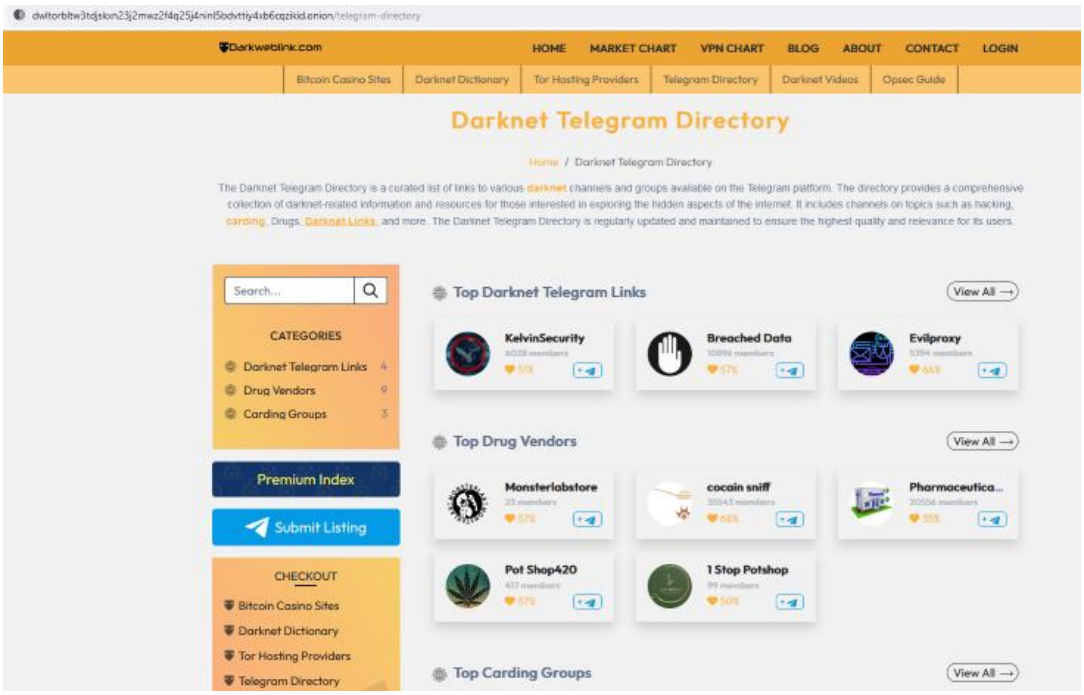


Imagen 123. Directorio de canales de Telegram detectados con TORCH

2.2.3. DEEP SEARCH

Deep Search es un buscador que permite realizar consultas dentro de la red Tor para descubrir contenido en dicha Darknet. En la Imagen 124 pueden verse que Deep Search tiene indexado un total de 315.135 sitios webs y ofrece una serie de estadísticas sobre el

top 10 de búsquedas en el propio Deep Search, yendo todo a la misma dinámica de búsquedas relacionadas con temas pornográficos.

El enlace es el siguiente: http://search7tdrcvri22rieiwgi5g46qnwsesvnubqav2xakhezv4hjzkkad.onion/

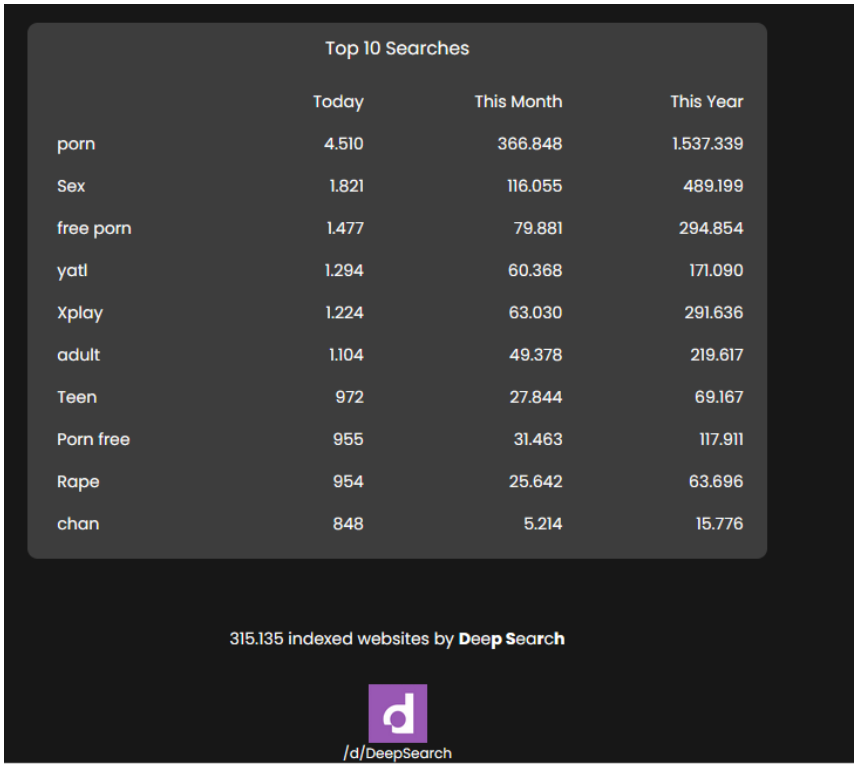


Imagen 124. Top 10 de búsquedas realizadas con Deep Search

Ahora, procedemos a realizar una consulta de la palabra clave "ransomware" dentro del buscador, el cual nos devuelve *15 resultados*. En la Imagen 125 se puede observar que obtenemos el título y una breve descripción de cada enlace .onion, junto con la URL asociada. Ahora se podría ir accediendo a cada enlace recolectado y descubrir si su contenido es interesante para la investigación o no.

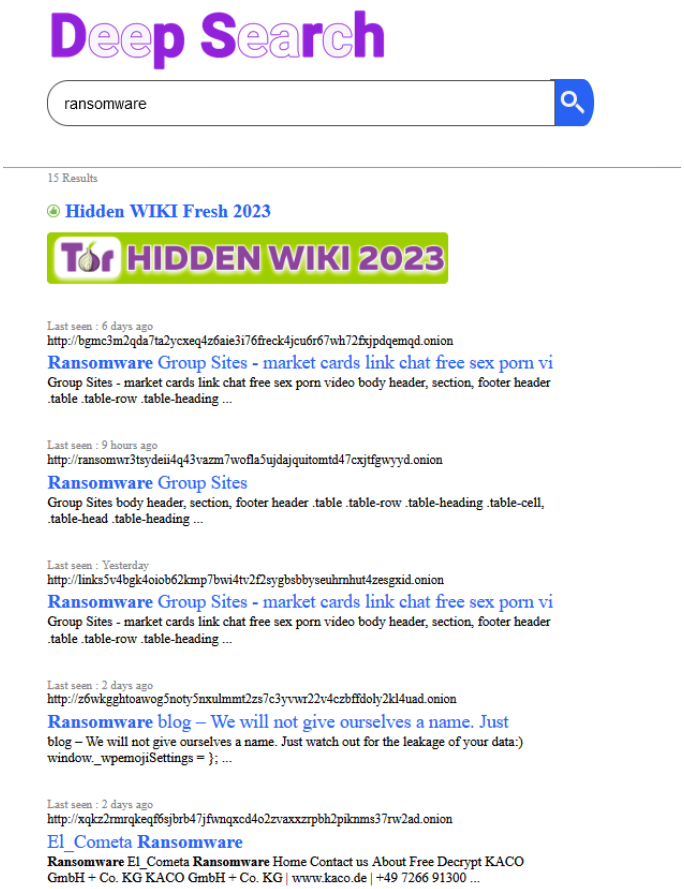


Imagen 125. Resultados de la palabra clave "ransomware" en Deep Search

2.2.4. THE DEEP SEARCHES

The Deep Searches es un buscador muy similar a los anteriores, el cual permite realizar consultas dentro de la red Tor para descubrir cualquier tipo de contenido. El enlace a The Deep Searches es el siguiente: http://searchgf7gdtauh7bhnbyed4ivxqmuoat3nm6zfrg3ymkq6mtnpye3ad.onion/.

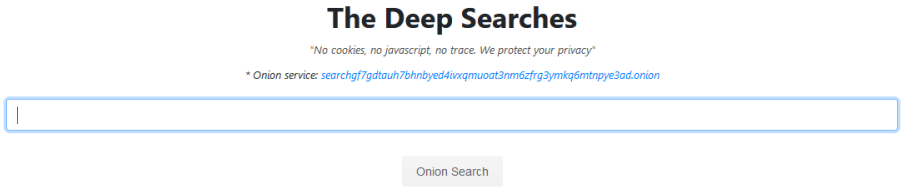


Imagen 126. Sitio web de The Deep Searches

En la Imagen 127 puede visualizarse los términos más utilizados como búsquedas dentro del buscador de The Deep Searches. El acceso al enlace hacia lo mencionado se puede encontrar a continuación: http://searchgf7gdtauh7bhnbyed4ivxqmuoat3nm6zfrg3ymkq6mtnpye3ad.onion/most-popular

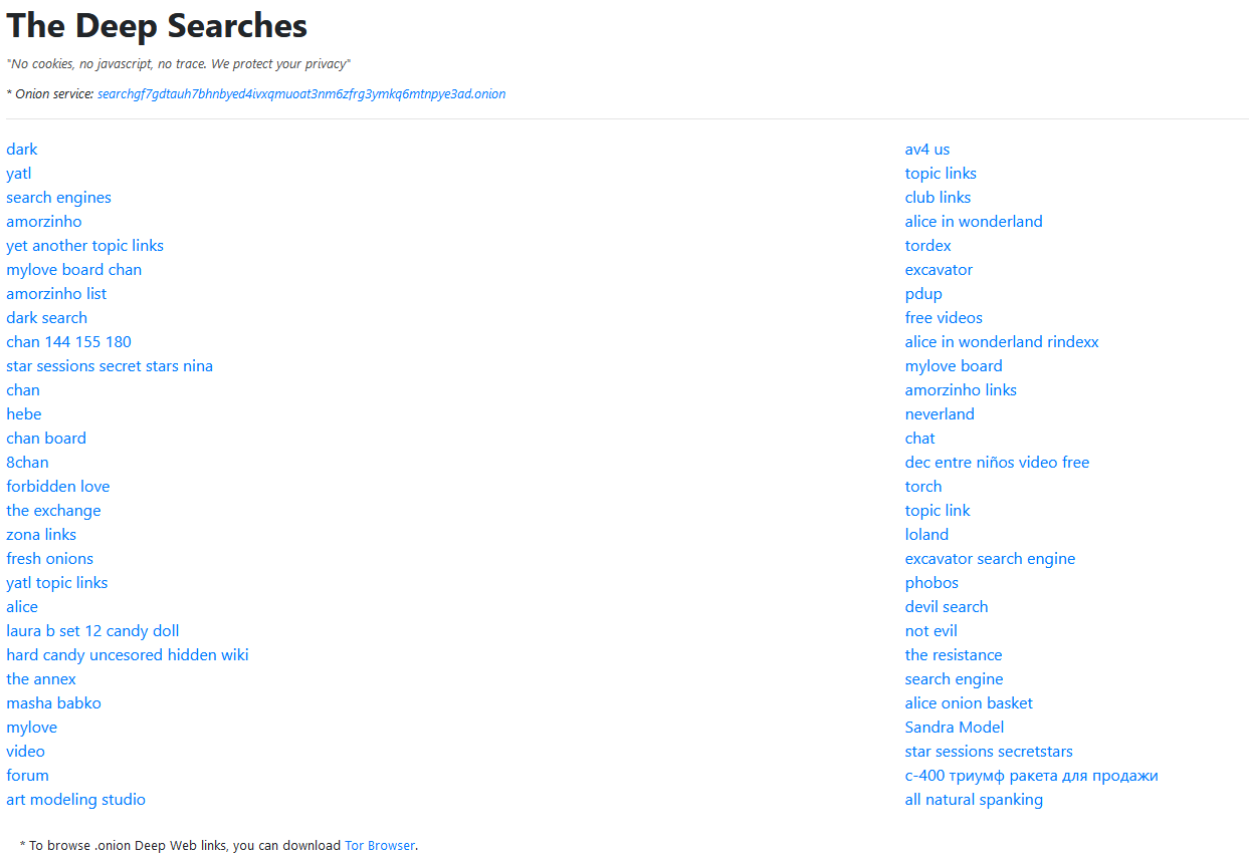


Imagen 127. Términos más utilizados como búsqueda dentro de The Deep Searches

Procedemos a realizar una consulta de la palabra clave "ransomware" dentro del buscador en conjunto con tres palabras clave a excluir (sex, xxx y porn). En la Imagen 128 pueden verse los resultados, obteniéndose un total de 133, donde cada uno de ellos aparece con su correspondiente enlace, título y descripción del sitio web.

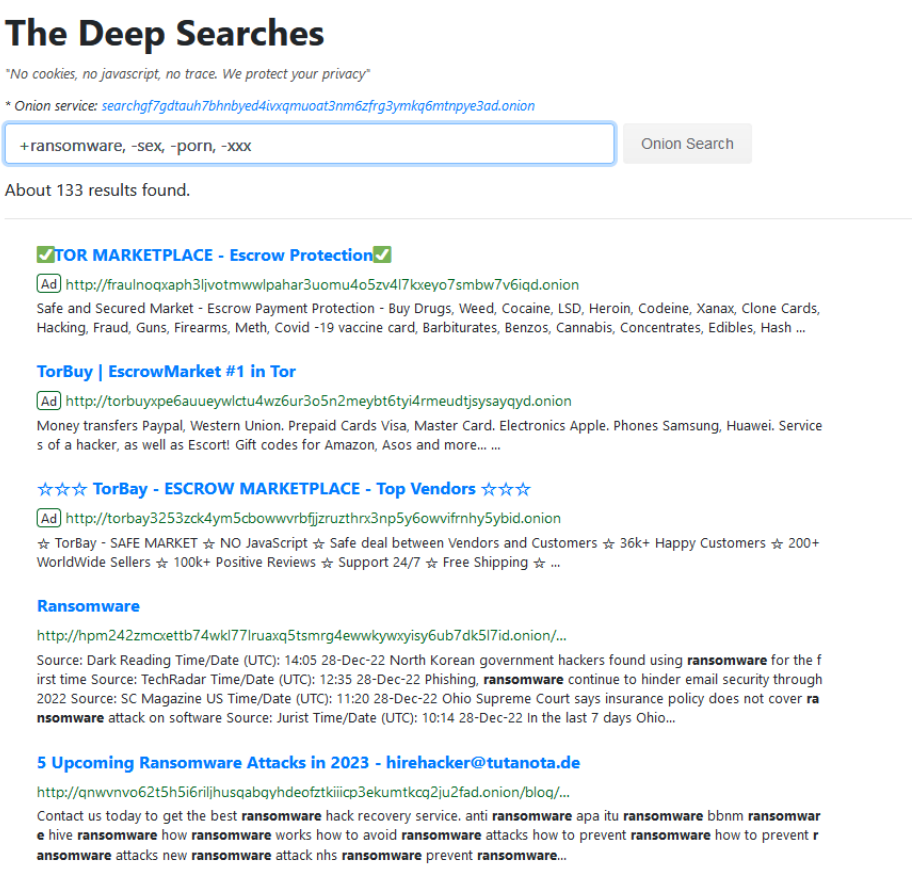


Imagen 128. Búsqueda de una dork con The Deep Searches