

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/tecnologia/2020/06/03/se-filtro-la-base-de-datos-de-uno-de-los-servicios-de-hosting-mas-grandes-de-la-dark-web/>.

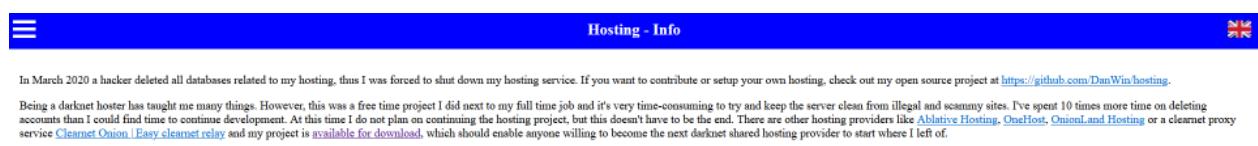


Imagen 95. Sitio web de Daniel Hosting indicando que ya no ofrece servicios de hosting en Tor

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>.

Language: čeština Deutsch English اسکرپت 日本語 Português Русский Türkçe

Test whether a Tor hidden service onion is online or offline

Onion link:

http://danielas3rtn54uwmofdo3x2

Test

Yes, the service is online!

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/>.

I'm not responsible for any content of websites linked here. 99% of darkweb sites selling anything are scams. Be careful and use your brain. I regularly receive E-Mails from people that were desperate to make money and fell for scammers, don't be one of them!

Onion address: http://onions.danwin1210.de

Description:

Category: All

Search term:

Category: Unsorted

Search term:

Search

Hide locked

Format: Text JSON

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.

Search:
ransomware

Category: All

Hide locked

Search

Searching for "ransomware", 1 results found:

Onion link	Description	Last seen	Added at	Actions
ransomwr3tavdeis4q43vazm7wofla5ujdasqu7omad47cxif5wyvd.onion	Ransomware Group Sites	2023-03-25 14:30	2022-12-27	Test

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: DBPbrvFShnykgBa3svQ91F9VgsizhhgmB1
 LTC: LKMDziBcT474Mava74r9BvkTygXcaUk6MD
 BTC/BCH: 1FyCD8kp9ekiTtgdyhFtZRgzR1QCHV4i84
 XMR: 48FgeW4fUpyjPDGxJdHaA441F5c9szYtLSVWbNv8T32Xe9ZN3iLUSSdASof2vDQqdbgRYom9aMeQMWPQkr3SP2UJE2uM8fc

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
CLOP	v3	Open
CONTI	v3	Open
CRYPTHONICOD3	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.

Search:

Category: Forums

Hide locked

Search

Searching for "", 8 results found:

Onion link	Description	Last seen	Added at	Actions
cebalks7umchbpeymasmp7pfos4maraxglkzre bz7x5rendphravdevel.onion	Cebalks - Polish .onion forum	2023-03-26 12:53	2018-12-19	Test
cr756qj2ukmuidf6o6wln5clq7227af7t0ome e73157bwlgq22dod.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
dreadsofinfoptof6q7l3xptbet6onoyno2vz7 jicokskvavbrad.onion	Dread - A popular forum	2023-03-27 06:17	2020-10-15	Test
eux4pt4caisnq5w7ppcencos5shapevycum s5yvnmoc4mcpc74ppvd.onion	AnonGTS	2023-03-27 02:32	2020-10-22	Test
g5pe3ue7ukerthdkccajx2sl5ih63ekaojk mcx267pnawpcyd.onion	XMundo - Turkiyah Dark Web Forum	2023-03-27 07:30	2023-03-11	Test
probiv7xf4357jp7byf572a3o37g25hdhbg7k gvpxey2corolsa4ad.onion	Форум по проблеме информации - probiv.cc	2023-03-26 18:06	2023-02-01	Test
thelhubce3bf6fpqdy4mxwd65d45emchim3x c53dpqsdna7m3qmknsmd.onion	The Hub - a popular forum	2023-03-21 19:38	2020-02-16	Test
thelhubce3bf6fpqdy4mxwd65d45emchim3x 7zgrwhbranfrwyd.onion	The Hub V3 Mirror List	2023-03-21 00:50	2020-02-23	Test

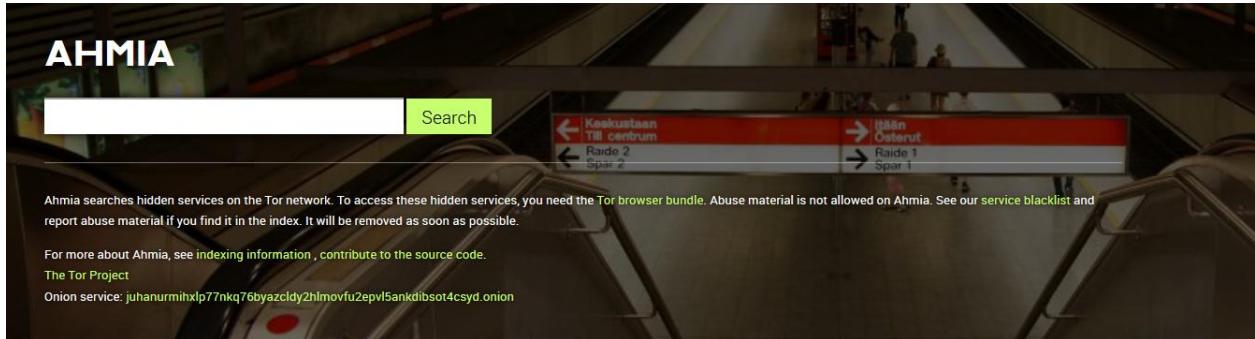
Imagen 100. Resultados de dominios .onion relacionados con foros

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://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibso4csyd.onion/>

**Imagen 101. Sitio web oficial de AHMIA**

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/>.

Linking graph of onions in our database
[Click here to visualize](#)

Usage Statistic Plots
[Click here to display](#)

For hidden service operators
You can add your domains and sub-domains on Ahmia add page: [Add](#)
Info about hidden service indexing and crawling: [Indexing](#)
Ahmia blacklists child abuse content: [Blacklist](#)

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

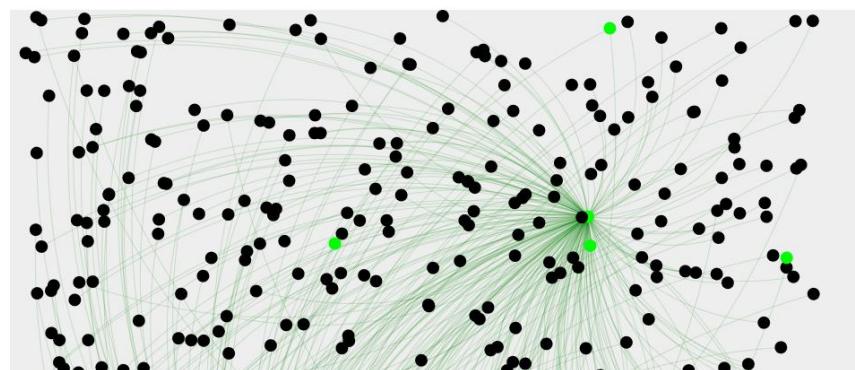
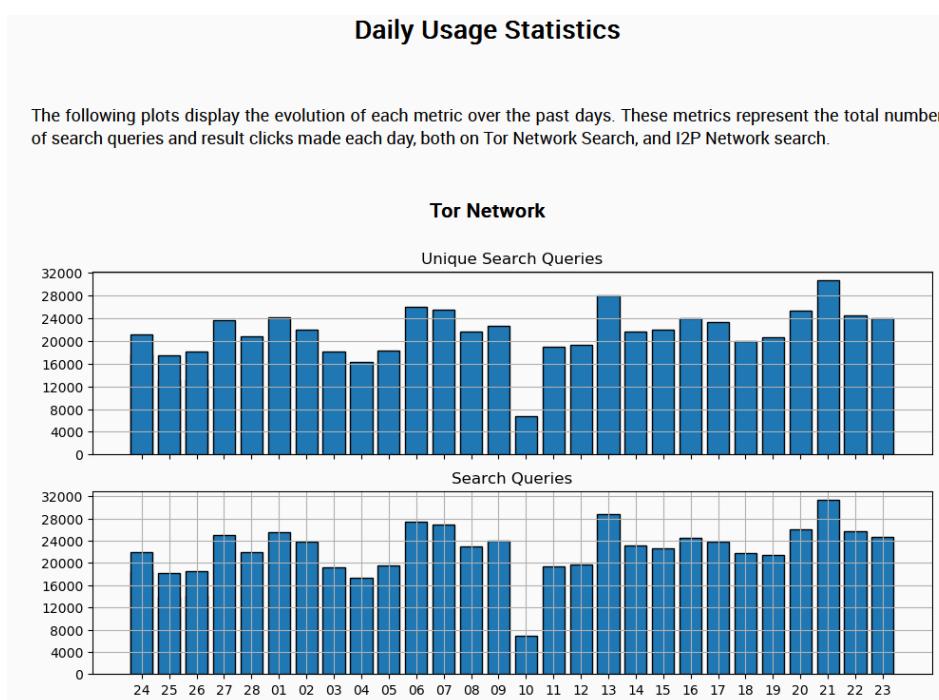


Imagen 103. Estadísticas de dominios .onion representados mediante grafos

**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.

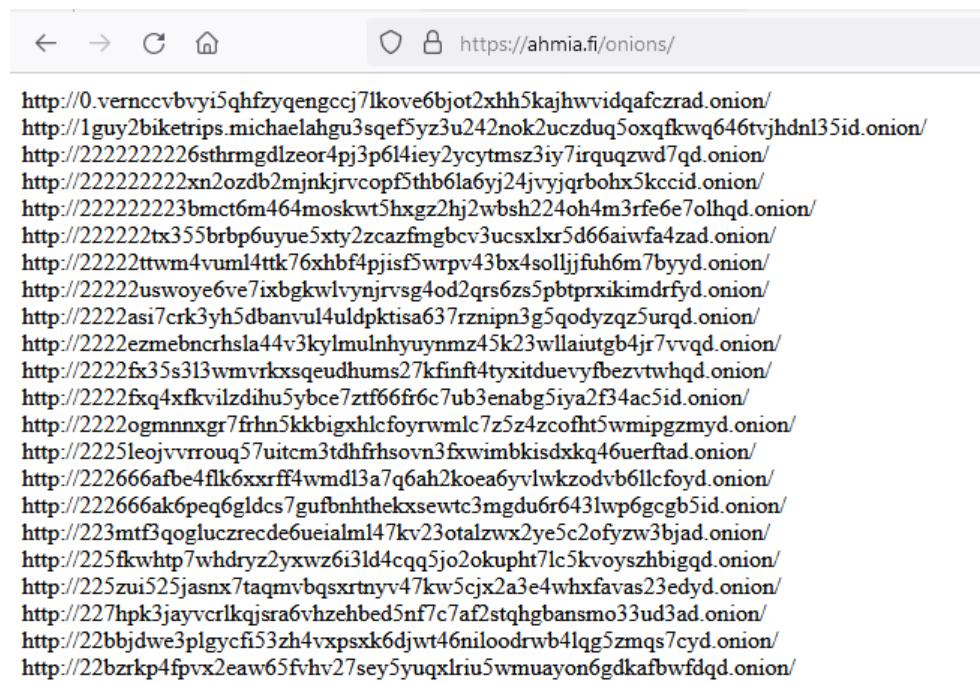


Imagen 105. Listado de dominios .onion indexados por AHMIA

- 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.

The screenshot shows the AHMIA search interface. The search bar contains 'ransomware'. Below the search bar are links for 'About Ahmia', 'Statistics', 'Add Service', and 'i2p search'. A green 'Search' button is on the right. The main area has a header 'Any Time ▾' and a note 'Omitted very similar entries. Displaying 236 matches in 0.62 seconds. Page 1 of 3.' Below this, several search results are listed as hyperlinks:

- [Ransomware Group Sites](#)
- [Ransomware – The Darkweb Marketplace](#)
- [Ransomware – Digital Thrift Shop](#)
- [Everest Ransomware Group](#)
- [October 2021 – Ransomware blog](#)
- [RANSOMWARE / Ransomware Builder Master / For begin - THE X WAVE MARKET](#)

Each result includes a brief description and a timestamp.

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/>

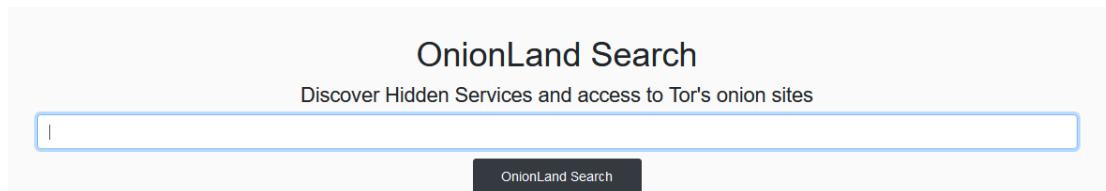


Imagen 107. Sitio Oficial de OnionLand

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://y2muyivq2fef2fmryi5up1...			27 Mar 2023
5002	http://bwazdcmukozwza37vljt...			27 Mar 2023
5003	http://b6ymwpjhqajg32k3o4o...			27 Mar 2023
5004	http://twister4lr6zox2lqfw2fnvn...	Twister News		27 Mar 2023
5005	http://wcn62ebohmmfyhmn...	Nikotile	Nikotile's personal website.	27 Mar 2023
5006	http://i7zp7y5dx6gh2dezwmtnb...			27 Mar 2023
5007	http://k3fszf3oymj3rimnmn35...	Monsterabstore 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://cardmen3iav7b5ecrmu...	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://2ml7jhg6sbp7emf5fsqj...			27 Mar 2023
5010	http://ad74f3en5e3tegrd5gwb...			27 Mar 2023

Imagen 108. Discover de Hidden Services de OnionLand

Most Popular Search Terms			
A	B	C	D
av4 us amorzinho list asian boys 11yo and 7yo have fun ... anal alice links anonfiles.com mp4 asian lolitas alice wonderland	amorzinho amorzinho links alice av4.us alina nikitina ass aiw abuse	alice in wonderland alice in wonderland rindexx art modeling studio as générateur de faux documents alina nikitina leaked photos annex art alice topic links 2.0	adult amateur girl photo all natural spanking alice basket anon image board alice in wonderland topic links av4 a
boys boy vids 6.0 boysland boy vids v4.0 boys club bonanza babko bank	boys r us boysvid 6.0 buy bitcoin credit card buy paypal account bitcoin baby bitcoin escrow buy	boys index page bestiality boy vids board black market buy iphone beastility black market...si...	boy blowjob bdsm black market guns buy gun boy chat boyvids boyvids 6.0
club links chat c-400 триумф cute russian girls - 8 yo strip and fi... cum computer chatango rooms candle search engine	chan 144 155 180 c-400 триумф ракета для продажи cloned cards cutie garden lg board spam cutie garden webm club crush fetish chemal and gegg	chan chat room carding dumpd cutie garden chatango mega chat rooms club link card	chan board credit card cute little 6 year olds candydoll credit cards candy cc 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.

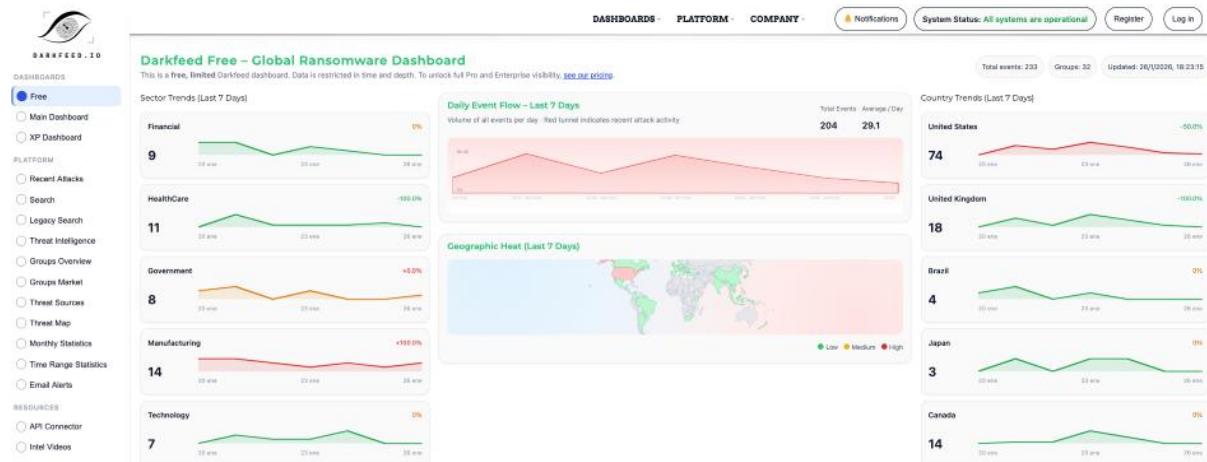


Imagen 110. Volumetrías sobre incidentes de ransomware ofrecidos por DarkFeed

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/>.

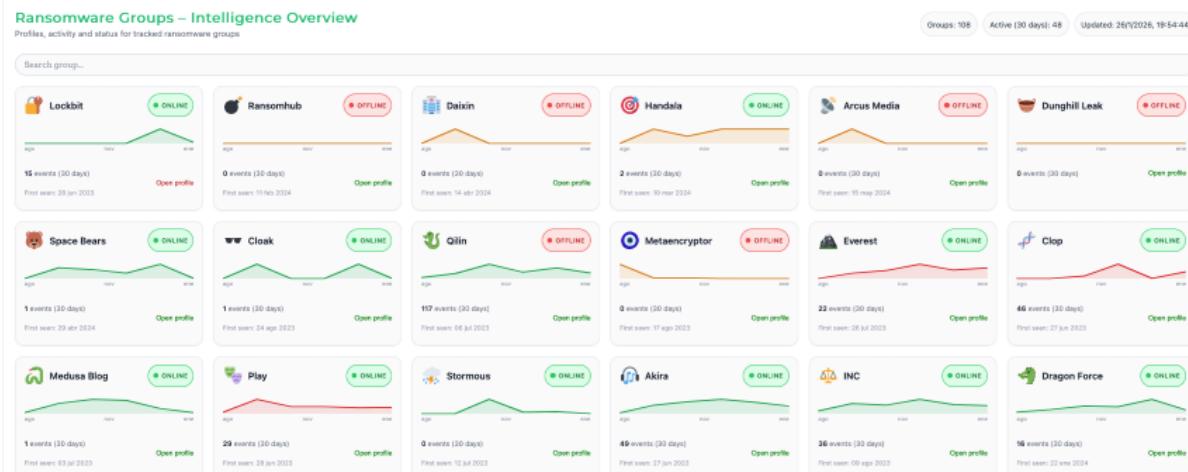


Imagen 111. Listado de grupos de ransomware en DarkFeed

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/>.

The screenshot shows the StealthMole website's 'Products' section. It features three dark-themed cards with white text. The first card, 'Darkweb Tracker', includes a shield icon, a brief description, and a 'Learn more →' button. The second card, 'Credential Protection', includes a lock icon, a brief description, and a 'Learn more →' button. The third card, 'Dark Web Monitoring', includes a magnifying glass icon, a brief description, and a 'Learn more →' button.

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.

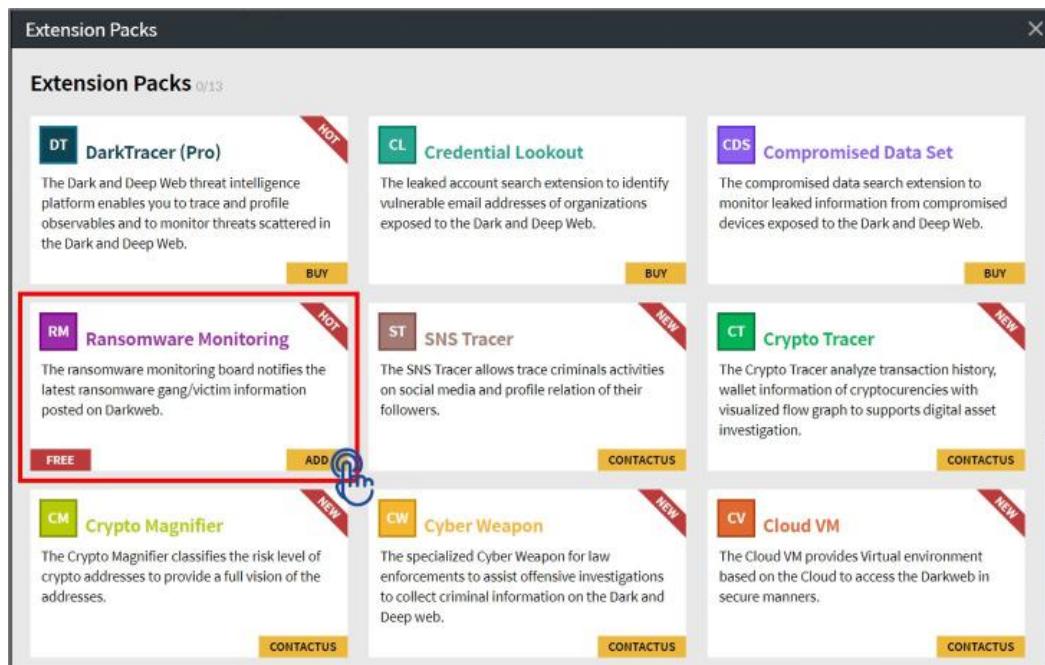


Imagen 114. Añadir modulo gratuito de StealthMole sobre ransomware

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.

Claimed Victim	Ransomware Gang	Detection Date (UTC+0)	Ransomware URL	Victim Site	Victim Country	Industrial Sector
secures.in	LockBit	2023-03-24 13:42:39	Not supported to FREE version	secures.in	India	Management Services
Sun Pharmaceutical Industries Ltd.	BlackCat (ALPHV)	2023-03-24 13:48:58	Not supported to FREE version	suppharma.com	India	Chemical Producers
Tekla	BlackCat (ALPHV)	2023-03-24 13:48:58	Not supported to FREE version	tekla.com	Turkey	Transportation Equipment
IMAGINE360.COM	CLOP	2023-03-24 14:25:05	Not supported to FREE version	imagine360.com	USA	Insurance Carriers
CCAA	Mallox	2023-03-24 15:05:32	Not supported to FREE version	www.ccaa.com.br	Brazil	Educational Services
Tip Top Poultry	AvosLocker	2023-03-24 17:01:29	Not supported to FREE version	tiptoppoultry.com	USA	Food Products
Zeller	AvosLocker	2023-03-24 17:01:29	Not supported to FREE version	maneygordon.com	USA	Legal Services

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.

SEARCH RESULTS	RESULTS
Tor Domains	143 results with possible sexual exploitation were filtered out.
Tor URL	oaqmsgee6avqr... Sorad.onion
I2P Domain	digbssbibka4...sgoxqd.onion
I2P URL	cchnsane4n4...4nwad.onion
Domain (Desprob)	powerj7kmpzk...rijuyd.onion
URL (Deepweb)	vko4osalhud...m7did.onion
Domain (North Korea)	22222277xkg...uzelqd.onion
URL (North Korea)	brave4u7jjdb...2v72qd.onion
Domain	jab2didplow...ly7qd.onion
	btdigggink2p...mzfsyd.onion
	gsu74gl3cs...smmid.onion
	hackeoyrzjy3...6e4ryd.onion
	nrc2z7raejk...qexqad.onion

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.

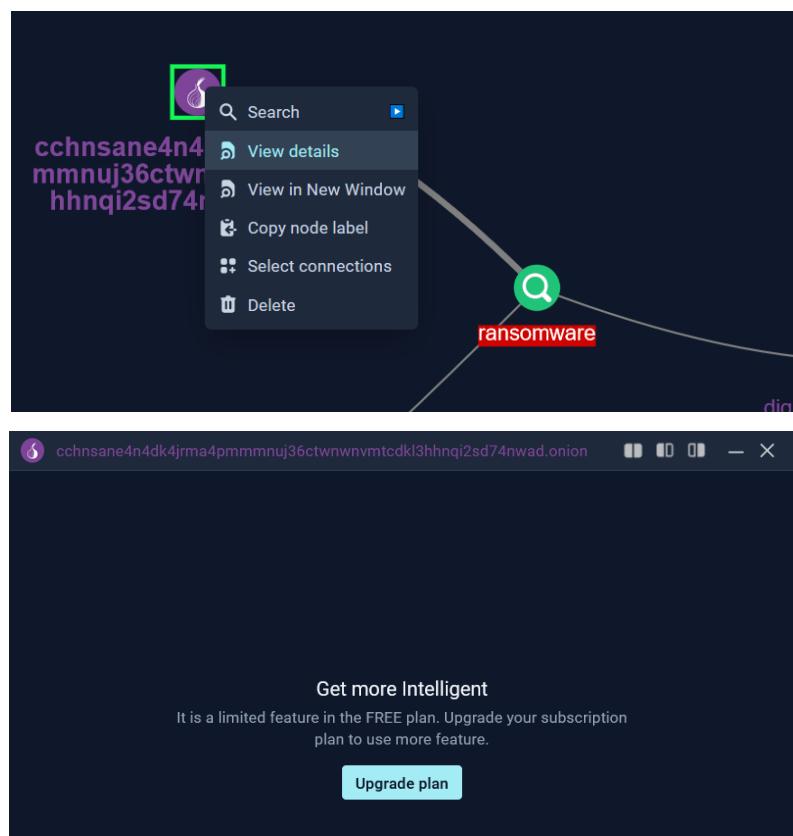


Imagen 117. Intento de ver detalle de un dominio añadido al grafo

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.

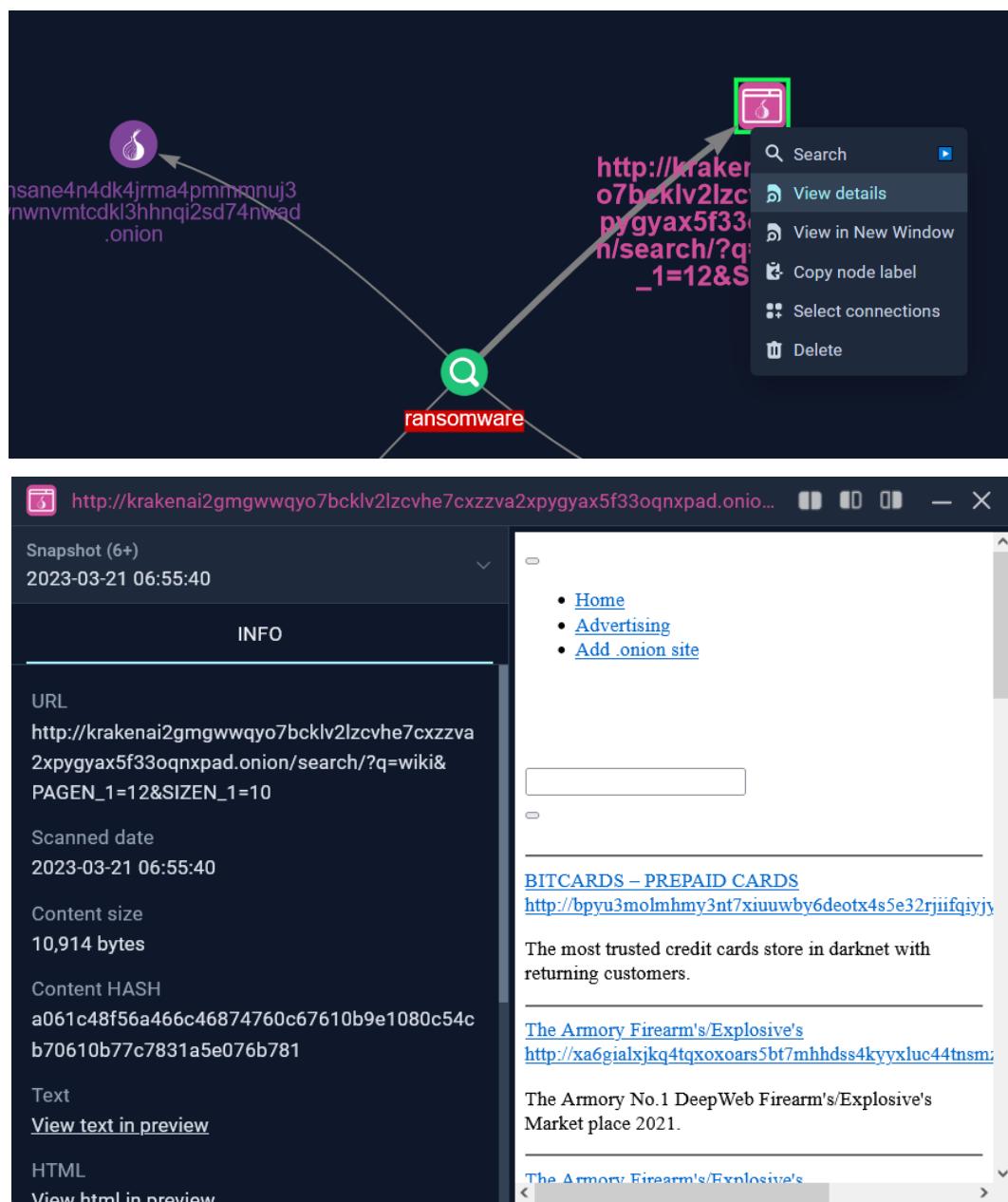


Imagen 118. Contenido de una URL de un dominio de Tor ofrecida por StealthMole

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://zqktlwiavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

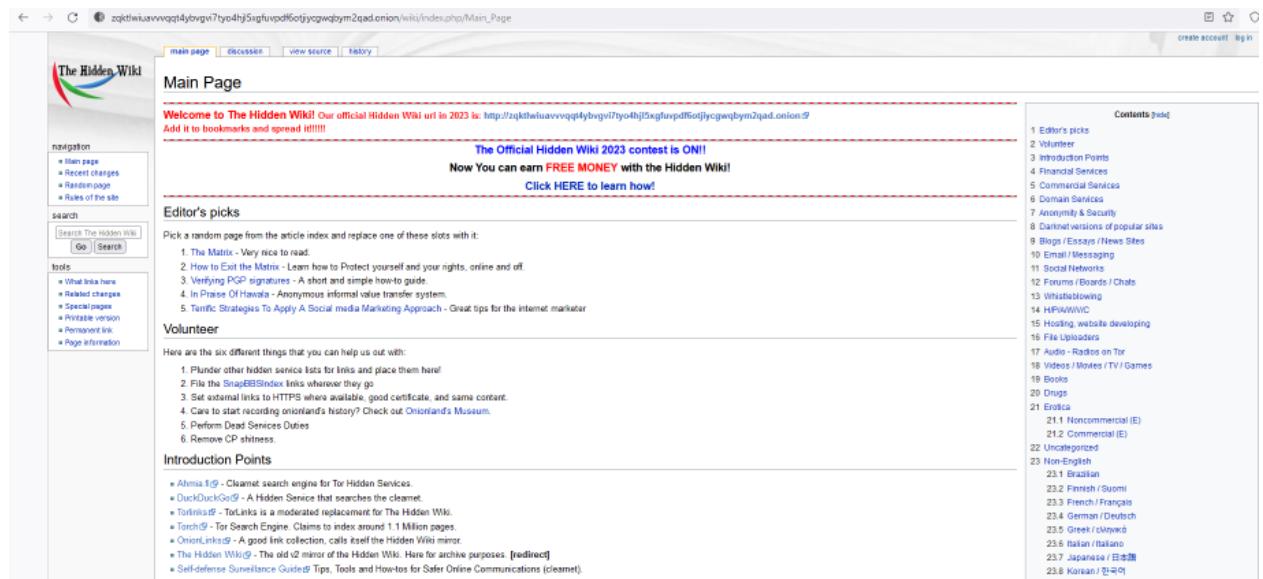


Imagen 119. Sitio web principal de The Hidden Wiki

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.

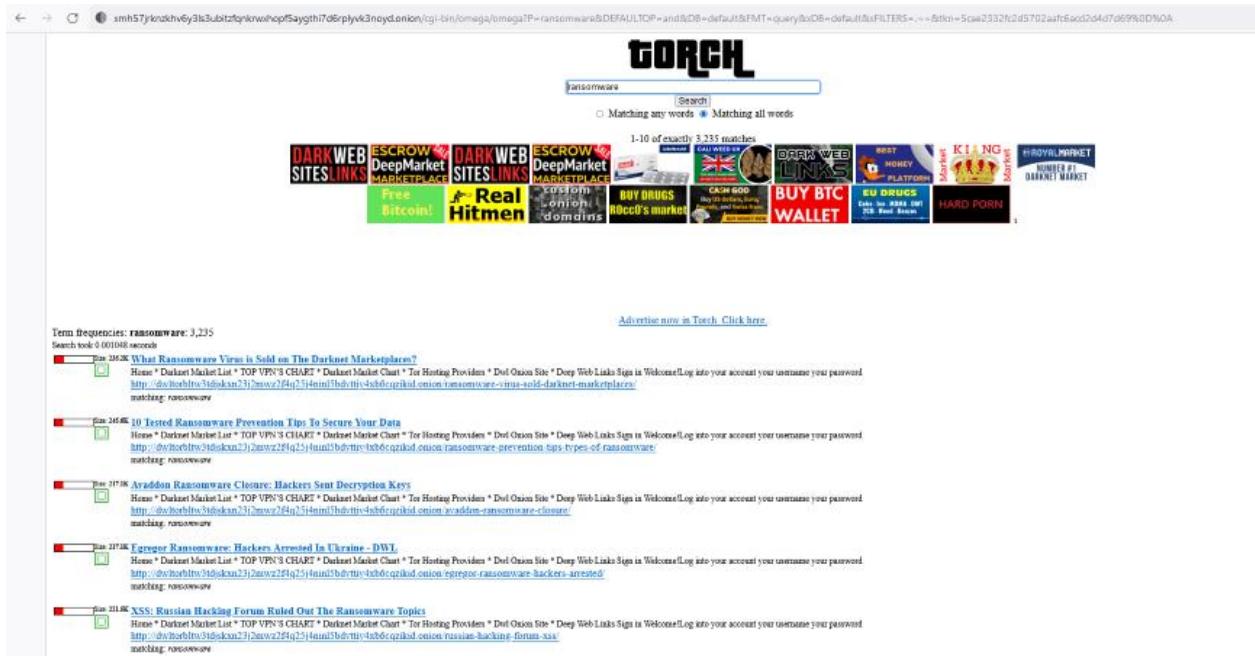


Imagen 121. Resultados de la palabra clave "ransomware" en TORCH

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)

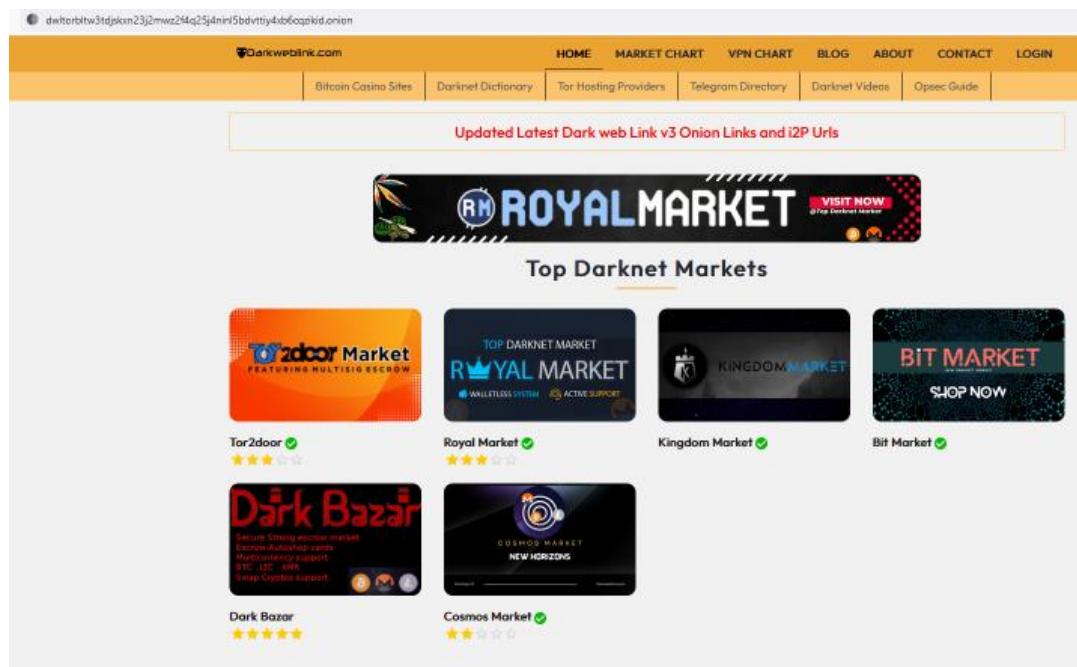


Imagen 122. Sitio web en Tor descubierto con TORCH

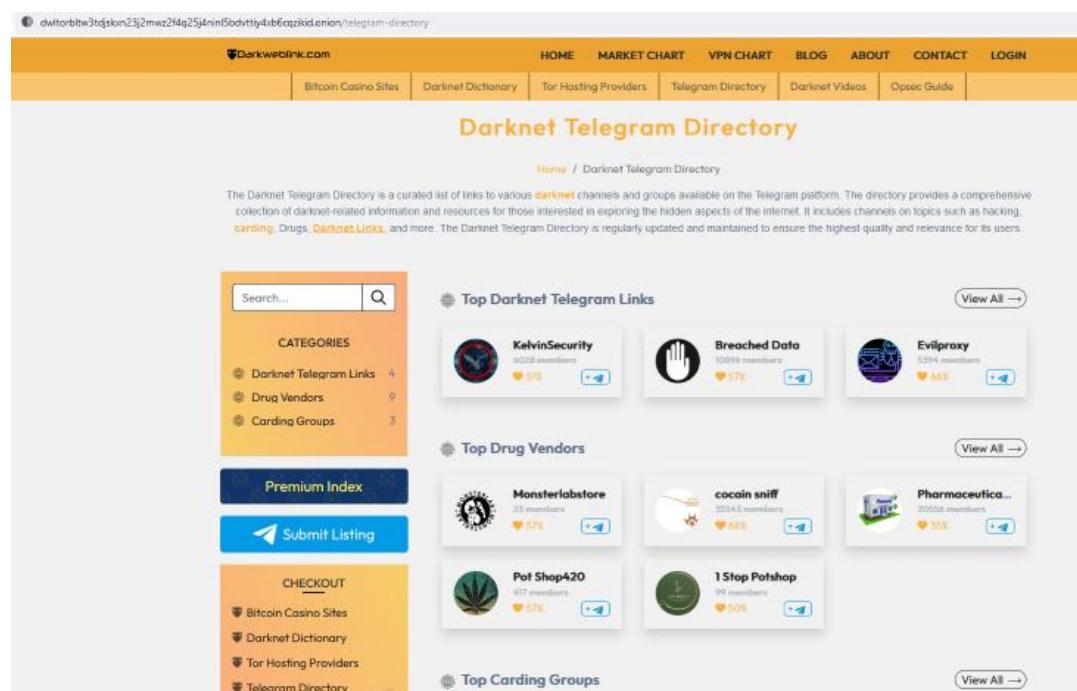


Imagen 123. Directorio de canales de Telegram detectados con TORCH

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://search7tdrcvri22rieiwd5g46qnwsesvnubqav2xakhezv4hjzkkad.onion/>

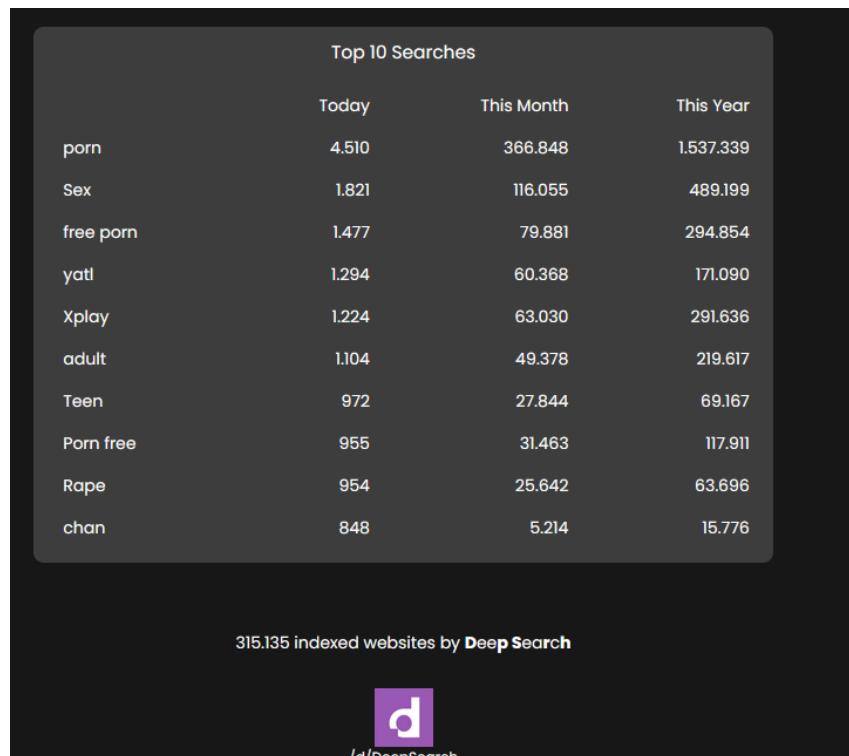


Imagen 124. Top 10 de búsquedas realizadas con Deep Search

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.

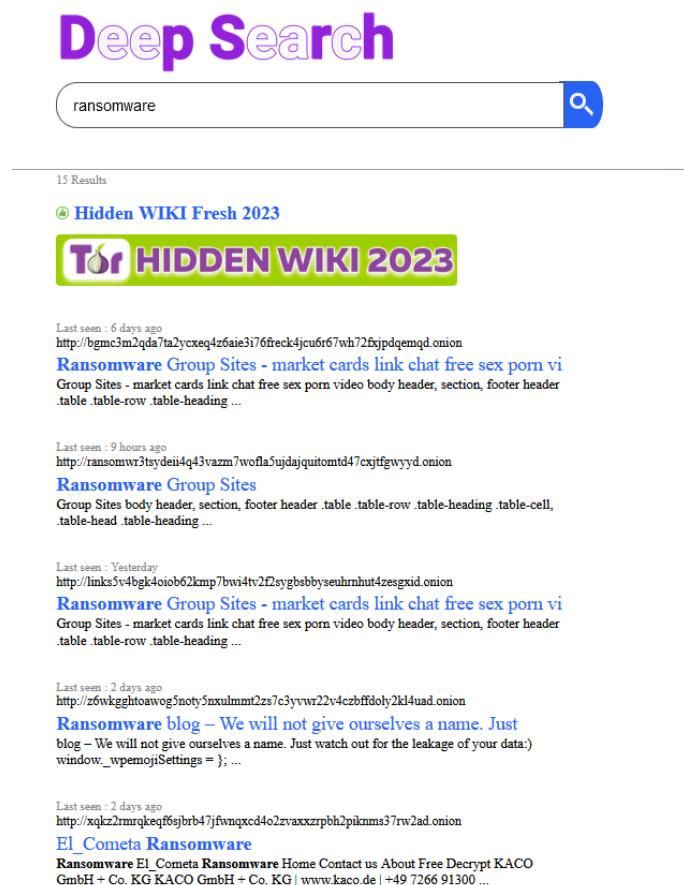


Imagen 125. Resultados de la palabra clave "ransomware" en Deep Search

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://searchg7gdtauh7bhnbyed4ivxqmuoat3nm6zfrg3ymkq6mtnpye3ad.onion/>.

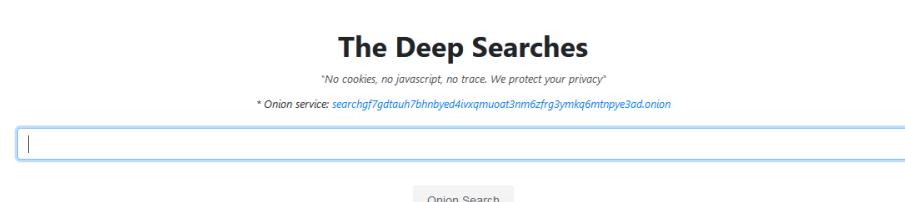


Imagen 126. Sitio web de The Deep Searches

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://searchgf7gdtauh7bhnbyed4ivxqmuat3nm6zfrg3ymkq6mtnpye3ad.onion/most-popular>

The Deep Searches

"No cookies, no javascript, no trace. We protect your privacy"

* Onion service: searchgf7gdtauh7bhnbyed4ivxqmuat3nm6zfrg3ymkq6mtnpye3ad.onion

dark	av4 us
yatl	topic links
search engines	club links
amorzinho	alice in wonderland
yet another topic links	tordex
mylove board chan	excavator
amorzinho list	pdup
dark search	free videos
chan 144 155 180	alice in wonderland rindexx
star sessions secret stars nina	mylove board
chan	amorzinho links
hebe	neverland
chan board	chat
8chan	dec entre niños video free
forbidden love	torch
the exchange	topic link
zona links	loland
fresh onions	excavator search engine
yatl topic links	phobos
alice	devil search
laura b set 12 candy doll	not evil
hard candy uncesored hidden wiki	the resistance
the annex	search engine
masha babko	alice onion basket
mylove	Sandra Model
video	star sessions secretstars
forum	c-400 триумф ракета для продажи
art modeling studio	all natural spanking

* To browse .onion Deep Web links, you can download Tor Browser.

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.

The Deep Searches

"No cookies, no javascript, no trace. We protect your privacy"

* Onion service: searchgf7gdtauh7bhnbyed4ivxqmuat3nm6zfrg3ymkq6mtrpye3ad.onion

+ransomware, -sex, -porn, -xxx

Onion Search

About 133 results found.

✓TOR MARKETPLACE - Escrow Protection✓

[Ad] <http://fraulnoqraph3ljvotmwlpahar3uomu4o5zv4l7kxeyo7smbw7v6iqd.onion>

Safe and Secured Market - Escrow Payment Protection - Buy Drugs, Weed, Cocaine, LSD, Heroin, Codeine, Xanax, Clone Cards, Hacking, Fraud, Guns, Firearms, Meth, Covid -19 vaccine card, Barbiturates, Benzos, Cannabis, Concentrates, Edibles, Hash ...

TorBuy | EscrowMarket #1 in Tor

[Ad] <http://torbuyxpe6auueywlctu4wz6ur3o5n2meybt6tyi4rmeudtjsysayqd.onion>

Money transfers Paypal, Western Union. Prepaid Cards Visa, Master Card. Electronics Apple. Phones Samsung, Huawei. Service s of a hacker, as well as Escort! Gift codes for Amazon, Asos and more... ...

☆☆☆ TorBay - ESCROW MARKETPLACE - Top Vendors ☆☆☆

[Ad] <http://torbay3253zck4ym5cbowwrbfjjrzuzthr3np5y6owvifrnhy5ybid.onion>

☆ TorBay - SAFE MARKET ☆ NO JavaScript ☆ Safe deal between Vendors and Customers ☆ 36k+ Happy Customers ☆ 200+ WorldWide Sellers ☆ 100k+ Positive Reviews ☆ Support 24/7 ☆ Free Shipping ☆ ...

Ransomware

[http://hpm242zmcttbb74wkl77lruaxq5tsmrg4ewwwkywxisy6ub7dk5l7id.onion/...](http://hpm242zmcttbb74wkl77lruaxq5tsmrg4ewwwkywxisy6ub7dk5l7id.onion/)

Source: Dark Reading Time/Date (UTC): 14:05 28-Dec-22 North Korean government hackers found using **ransomware** for the first time Source: TechRadar Time/Date (UTC): 12:35 28-Dec-22 Phishing, **ransomware** continue to hinder email security through 2022 Source: SC Magazine US Time/Date (UTC): 11:20 28-Dec-22 Ohio Supreme Court says insurance policy does not cover **ransomware** attack on software Source: Jurist Time/Date (UTC): 10:14 28-Dec-22 In the last 7 days Ohio...

5 Upcoming Ransomware Attacks in 2023 - hirehacker@tutanota.de

[http://qnwwnvo62t5h5i6rlijhusqabqyhdeofztktiiicp3ekumtkcq2ju2fad.onion/bloq/...](http://qnwwnvo62t5h5i6rlijhusqabqyhdeofztktiiicp3ekumtkcq2ju2fad.onion/bloq/)

Contact us today to get the best **ransomware** hack recovery service, anti **ransomware** apa itu **ransomware** bbnm **ransomware** hive **ransomware** how **ransomware** works how to avoid **ransomware** attacks how to prevent **ransomware** how to prevent **ransomware** attacks new **ransomware** attack nhs **ransomware** prevent **ransomware**...

Imagen 128. Búsqueda de una dork con The Deep Searches