(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 719 123**

(21) Número de solicitud: 201831145

(51) Int. CI.:

G06F 16/95 (2009.01)
G06F 16/951 (2009.01)
G06F 16/9538 (2009.01)

(12) PATENTE DE INVENCIÓN CON EXAMEN B2

(22) Fecha de presentación:

26.11.2018

(43) Fecha de publicación de la solicitud:

08.07.2019

Fecha de concesión:

03.09.2020

(45) Fecha de publicación de la concesión:

10.09.2020

(73) Titular/es:

UNIVERSIDAD DE LEÓN (100.0%)
Avenida de La Facultad 25
24071 León (León) ES

(72) Inventor/es:

MHD WESAM , Al-nabki ;
FIDALGO FERNÁNDEZ, Eduardo;
ALEGRE GUTIÉRREZ , Enrique y
FERNÁNDEZ ROBLES , Laura

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

(54) Título: **PROCEDIMIENTO Y SISTEMA PARA LA CLASIFICACIÓN Y DETECCIÓN DE LOS DOMINIOS MÁS INFLUYENTES DENTRO DE LA RED OSCURA TOR**

(57) Resumen:

Procedimiento y sistema para la clasificación y detección de los dominios más influyentes dentro de la red oscura Tor (1). El procedimiento incluye rastrear y descargar texto en bruto (3) de un dominio (7), mediante un ordenador (2) conectado a internet; obtener un fichero HTML (4) a partir del texto en bruto (3); preprocesar el texto en bruto (5) para obtener un texto preprocesado (6) con hipervínculos entrantes y salientes del dominio (7); realizar una clasificación automática (6a) del texto preprocesado (6) mediante vectores de características y un algoritmo de aprendizaje automático basado en regresión, y obtener una serie de categorías de dominios (6b); construir un grafo de actividades de interés (8) con los hipervínculos entrantes y salientes; determinar el valor de rango (9) para cada dominio, obtenido ponderando la suma de enlaces de cada nodo; realizar una ordenación de los nodos; etiquetar los dominios más influyentes.

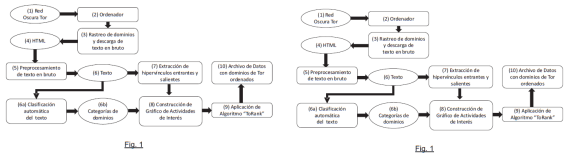

Fig. 1

ES 2 719 123 B2

DESCRIPCIÓN

PROCEDIMIENTO Y SISTEMA PARA LA CLASIFICACIÓN Y DETECCIÓN DE LOS DOMINIOS MÁS INFLUYENTES DENTRO DE LA RED OSCURA TOR

OBJETO DE LA INVENCIÓN

El objeto de la presente invención es un procedimiento y sistema automatizado para clasificar y detectar los dominios más influyentes dentro de la red oscura Tor (The Onion Router) en función de los hipervínculos que contengan. La invención permite identificar qué dominio es el más influyente dentro de la red, es decir, el dominio cuya eliminación provocaría la mayor desestabilización de la red. Dicha desestabilización afectaría a una reducción muy elevada u obstrucción en la transmisión de información a través de los diferentes dominios. Esta invención, también permite identificar las categorías de los diferentes dominios analizados, e identificar el dominio más influyente por categoría.

ANTECEDENTES DE LA INVENCIÓN

En la actualidad, el modo de acceder a la información en Internet es a través del uso de motores de búsqueda, como Google o Bing. A pesar de que son eficientes y muy potentes, no pueden indexar todo el contenido de la Web. El contenido que está indexado pertenece a la Web Superficial, y resto del contenido, que no está indexado, pertenece a la Web Profunda. Dentro de la Web Profunda, hay una parte formada por varias redes y se denomina Red Oscura, siendo Tor (The Onion Router) la red oscura más famosa, debido al nivel de anonimidad que proporciona a sus usuarios.

Debido a la topología de Tor y al hecho de que no es posible registrar el tráfico de los dominios, no es posible establecer una medición de la popularidad o influencia de dichos dominios dentro de la red. Además, dada la anonimidad que proporciona, la red oscura Tor aloja dominios con diferentes contenidos, tanto legales como ilegales. A raíz del contenido ilegal de Tor, surge la necesidad de clasificar dicho contenido en diferentes tipos de actividades ilegales e identificar qué dominios son los más influyentes dentro de la red, tanto a nivel global como para cada categoría. La eliminación de los dominios más influyentes desestabilizaría la red y dificultaría la transmisión de información a través de los diferentes dominios.

La clasificación manual de los dominios presenta una serie de inconvenientes. En primer lugar, debido al elevado número de posibles dominios, del orden de decenas de miles, se

requiere de una alta inversión de tiempo y personal para realizar la clasificación. Además, la clasificación depende en gran medida de la persona que la realiza, aportando subjetividad que genera una disparidad de criterio entre expertos. También, la clasificación de dominios no siempre es fiable, ya que frecuentemente se producen errores derivados por el cansancio y la falta de atención del experto. Por último, es un proceso costoso por los elevados costes asociados al tiempo de la persona que realiza la clasificación.

Debido a las anteriores características de la red oscura Tor, solo sería posible utilizar el contenido textual de sus dominios para realizar una medida de la influencia de los mismos, dado que determinados contenidos visuales serían ilegales según la normativa española, como la pornografía infantil. Teniendo en cuenta esta limitación, se recurre al análisis de la relevancia de los dominios basada en teoría de grafos, donde los dominios serán los nodos y los hipervínculos entre ellos los enlaces. Según varios estudios (K. Taha and P. Yoo, “Using the Spanning Tree of a Criminal Network for Identifying Its Leaders”, IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 445-453, 2017), para poder desestabilizar una red es necesario eliminar los nodos más influyentes del grafo, para así conseguir una reducción significativa del flujo de información a través del grafo.

La medición de la influencia o relevancia de los nodos dentro de un grafo empezó a utilizarse hace más de 60 años. Inicialmente se trabajó con medidas de centralidad (Bavelas, A. (1948). «A mathematical model for group structures». Human Organization 7: 16-30.), que con el tiempo fueron evolucionando a algoritmos más complejos, como Katz (Katz, L. (1953). A New Status Index Derived from Sociometric Analysis. Psychometrika, 39–43.), HIST (Jon M. Kleinberg. 1999. Hubs, authorities, and communities. ACM Comput. Surv. 31, 4es, Article 5, December 1999) o PageRank (US6285999B1, 1997).

A pesar de que los anteriores algoritmos de medición de influencia consiguen resultados aceptables a la hora de desestabilizar una red, no se ha descrito específicamente un método y un sistema para la clasificación y posterior detección de los dominios más influyentes en la red oscura Tor.

DESCRIPCIÓN DE LA INVENCIÓN

El objeto de la presente invención es un procedimiento y sistema automatizado para clasificar y detectar los dominios más influyentes dentro de la red oscura Tor (The Onion Router) en

función de los hipervínculos que existan entre ellos. Los hipervínculos son, por tanto, propios de los dominios.

El procedimiento y sistema para la clasificación y detección de los dominios más influyentes dentro de la red oscura Tor (The Onion Router) de la presente invención permite clasificar y ordenar automáticamente grandes repositorios de dominios obtenidos mediante tecnología digital (ordenador) con acceso a internet, y conectado a la red Tor para recopilar información textual.

La clasificación automática, como paso intermedio a la detección de dominios influyentes, frente a la manual por un experto anula la subjetividad, los errores por cansancio y falta de atención, la disparidad de criterio entre expertos, los costes asociados al tiempo del experto, disminuye el tiempo necesario para la clasificación y aumenta la fiabilidad del etiquetado. Por este motivo, este procedimiento puede ser implementado en herramientas utilizadas por empresas y FFCCSSEE (Fuerzas y Cuerpos de Seguridad del Estado) para realizar una clasificación de los dominios de la red oscura Tor en diferentes categorías, y su posterior detección de los dominios más influyentes, tanto dentro de la red Tor como en cada categoría ilegal seleccionada.

La presente invención puede ser también aplicada en el entrenamiento o aprendizaje a distancia de personal especializado en las diferentes categorías consideradas como ilegales. La disposición de grandes conjuntos de dominios ya clasificados y las posibilidades actuales para recolectar nuevos dominios y enviarlos a un sistema de forma remota, permitiría que personal de FFCCSSEE o de empresa mejoren su conocimiento sobre las diferentes categorías ilegales presentes en la red oscura Tor, lo que aumentaría su conocimiento a la hora de diferenciarlas de otras categorías legales presentes en dicha red.

Dentro del proceso previo al procedimiento de la invención, el sistema permitiría realizar la clasificación automática de dominios mediante la codificación de texto a través de la Frecuencia de Términos – Frecuencia Inversa del Documento (TF-IDF, “Term Frequency – Inverse Document Frequency), métrica que indica la relevancia de una palabra en un documento, y su posterior clasificación con Regresión Logística (LR, “Logistic Regression”). Los dominios clasificados pertenecen a las siguientes categorías: (i) pornografía, (ii) criptomoneda, (iii) contrabando de tarjetas de crédito, (iv) venta de drogas ilegales, (v) actividades violentas, (vi) ataques cibernéticos (hacking), (vii) falsificación de moneda, (viii)

contrabando de identificación personal y (ix) otros.

A continuación, el procedimiento de la invención permite realizar la medida de la influencia de los dominios ilegales tanto (i) a nivel global como (ii) a nivel de cada una de las categorías anteriores. Para ello se construye un Grafo de Actividades Interesantes, donde cada dominio es representado por un nodo, y los enlaces del grafo provienen de los diferentes hipervínculos entrantes y salientes contenidos en los anteriores dominios. Por tanto, los enlaces son propios de los nodos y existen tantos enlaces entrantes al nodo como hipervínculos le apuntan a él y tantos enlaces salientes del nodo como él apunta a otros hipervínculos. En este proceso se eliminan los enlaces duplicados, es decir, aquellos que tienen el mismo origen y destino, para evitar la creación de multigrafos, y también aquellos enlaces a la Web Superficial. A continuación, se aplica el algoritmo que permite identificar cuales son los dominios más influyentes dentro de toda la red, y también por cada categoría, cuya eliminación afectaría al flujo de información dentro de la red.

En una realización preferente de la invención, este procedimiento se aplica a dominios ilegales de la red Tor, tanto a nivel global como por las diferentes categorías, aunque se puede aplicar sin realizar la categorización de actividades ilegales. También se puede extender a dominios legales de la misma red, a su aplicación en la Web Superficial, a redes de contactos y, en general, a cualquier tipo de red donde haya enlaces entrantes y salientes entre sus diferentes elementos.

En la presente descripción, antes de codificar el texto para su posterior clasificación, este es preprocesado. Tras un rastreo de todos los dominios de Tor, se descargan los recursos de aquellos que están activos y se extrae su fichero HTML. A continuación, se seleccionan aquellos dominios que están en inglés y se eliminan las etiquetas del lenguaje HTML, caracteres especiales y palabras vacías. En la presente invención, el término “texto en bruto” se refiere al que está contenido en el HTML del dominio y donde no se ha aplicado ningún preprocesamiento. Por otro lado, se emplea de manera general el término “texto” para hacer referencia al texto resultante tras el preprocesamiento del “texto en bruto” según la anterior descripción.

El procedimiento preferible para la clasificación y posterior detección de los dominios ilegales más influyentes dentro de la red oscura Tor de la presente invención comprende las siguientes etapas:

1. Rastreo de dominios y descarga de texto en bruto. A partir de una lista pública de dominios de la red Tor, se rastrean dichos dominios y se descarga, para cada dominio que esté activo en el momento del rastreo, su fichero HTML, el cual contiene el texto en bruto. Este rastreo y descarga de dominios se hace a través de un ordenador con conexión a internet y a la red oscura Tor.

2. Preprocesamiento de texto en bruto: dentro del mismo ordenador, para cada fichero HTML obtenido se realiza el preprocesamiento del texto bruto contenido para obtener el texto. A continuación, y de acuerdo con una realización preferente de la invención, a través de una librería de detección de idioma se seleccionan aquellos dominios que están en inglés, con el objeto de mejorar el posterior entrenamiento del sistema de clasificación, al ser el inglés el lenguaje mayoritariamente usado en la red Tor. En una realización preferente se eliminan las etiquetas del lenguaje HTML, caracteres especiales y palabras vacías, dando lugar al texto final.

3. Clasificación del texto: de acuerdo con una realización preferente de la invención, se realiza un proceso de clasificación automática del texto, con el objeto de poder identificar cuáles serán los dominios más influyentes de la red oscura Tor dentro de cada una de las categorías de actividades ilegales que contiene. En una realización preferente, se codifica el texto con la Frecuencia de Términos – Frecuencia Inversa del Documento (TF-IDF, “Term Frequency – Inverse Document Frequency”) y se clasifican los dominios con Regresión Logística (LR, “Logistic Regression”) en las siguientes categorías: (i) pornografía, (ii) criptomoneda, (iii) contrabando de tarjetas de crédito, (iv) venta de drogas ilegales, (v) actividades violentas, (vi) ataques cibernéticos (hacking), (vii) falsificación de moneda, (viii) contrabando de identificación personal y (ix) otros. De acuerdo con una realización preferente de la invención, para la Frecuencia de Términos – Frecuencia Inversa del Documento se utiliza una longitud de vector mínima de tres y máxima de 10000 elementos, y para la clasificación con Regresión Logística se activó el balance de pesos entre clases.

4. Construcción del Grafo de Actividades Interesantes: una vez tenemos el texto preparado, se construye el Grafo de Actividades Interesantes para todos los dominios de la red Tor. En una realización preferente de la invención, también se construyen los Grafos de Actividades Interesantes correspondientes a los dominios clasificados en las nueve categorías indicadas previamente. En dicha realización preferente, se asocia cada dominio a los nodos del grafo y los enlaces entre los diferentes nodos se establecen en función de los hipervínculos

entrantes y salientes de cada dominio. En la realización preferente, se eliminan los hipervínculos duplicados, es decir, aquellos que tienen el mismo origen y destino.

5. Cálculo de dominios más influyentes con algoritmo de influencia. Por último, se procede al cálculo de los dominios más influyentes de la red oscura Tor. De acuerdo con una realización preferente de la invención, también se calculan los dominios más influyentes de las diferentes categorías ilegales la red oscura Tor para los que se generaron los anteriores Grafos de Actividades de Interés. Dicho cálculo se lleva a cabo en dos fases. En una primera fase, se aplica el algoritmo de influencia, el algoritmo de medida de la influencia de dominios para calcular el ranking de los diferentes dominios extraídos de la red Tor. El valor de rango de un dominio se obtiene como la combinación ponderada de la suma del número de hipervínculos de los dominios seguidores y seguidos del dominio analizado. Según varios estudios, la desestabilización de una red se consigue eliminando los nodos con un mayor ranking, lo que da lugar a una obstrucción en el flujo de la información a través del grafo. De acuerdo con una realización preferente de la invención, se interpreta la influencia dentro de la red oscura Tor como la cantidad de obstrucción que un nodo puede causar al Grafo de Actividades Interesantes cuando es eliminado. En una segunda fase, se realiza una ordenación descendente de dichos dominios según el valor de rango obtenido, siendo los primeros dominios los de mayor valor y por lo tanto considerados los más influyentes.

Un segundo aspecto de la presente invención se refiere a un sistema para la clasificación y posterior detección de los dominios ilegales más influyentes dentro de la red oscura Tor a partir de dominios recuperados de la red oscura Tor. El sistema comprende medios de procesamiento de datos, tales como un ordenador con conexión a internet, configurado para rastrear y descargar el texto en bruto o HTML de dominios de la red Tor; preprocesar el texto en bruto para obtener texto preparado para ser analizado; realizar una clasificación automática (opcional) de dichos dominios mediante Frecuencia de Términos – Frecuencia Inversa del Documento y Regresión Logística; generar un Grafo de Actividades de Interés, siendo los nodos los dominios y los enlaces los hipervínculos entre los diferentes dominios; aplicar el algoritmo de influencia para obtener los dominios más influyentes dentro de la red Tor, siendo aquellos que obtienen el mayor valor del algoritmo.

En una realización preferente de la invención, el sistema comprende un ordenador conectado a internet y con acceso configurado a la red oscura Tor. El sistema también puede comprender unos medios de almacenamiento de datos donde se almacenan archivos HTML o texto en

bruto, archivos conteniendo el texto preprocesado, las categorías de los dominios, los Grafos de Actividades de Interés y la ordenación de los dominios de la red Tor ordenados según el valor de rango.

Por último, la presente invención también se refiere a un producto de programa que comprende medios de instrucciones de programa para llevar a la práctica el procedimiento anteriormente descrito cuando el programa se ejecuta en un procesador. El producto de programa está preferentemente almacenado en un medio de soporte de programas. Los medios de instrucciones de programa pueden tener la forma de código fuente, código objeto, una fuente intermedia de código y código objeto, por ejemplo, como en forma parcialmente compilada, o en cualquier otra forma adecuada para uso en la puesta en práctica de los procesos según la invención.

El medio de soporte de programas puede ser cualquier entidad o dispositivo capaz de soportar el programa. Por ejemplo, el soporte podría incluir un medio de almacenamiento, como una memoria ROM, una memoria CD ROM o una memoria ROM de semiconductor, una memoria flash, un soporte de grabación magnética, por ejemplo, un disco duro o una memoria de estado sólido (SSD, del inglés *solid-state drive*). Además, los medios de instrucciones de programa almacenados en el soporte de programa pueden ser, por ejemplo, mediante una señal eléctrica u óptica que podría transportarse a través de cable eléctrico u óptico, por radio o por cualquier otro medio.

Cuando el producto de programa va incorporado en una señal que puede ser transportada directamente por un cable u otro dispositivo o medio, el soporte de programa puede estar constituido por dicho cable u otro dispositivo o medio.

Como variante, el soporte de programa puede ser un circuito integrado en el que va incluido el producto de programa, estando el circuito integrado adaptado para ejecutar, o para ser utilizado en la ejecución de los procesos correspondientes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación, se describen de manera muy breve una serie de figuras que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta.

La Fig. 1 muestra un esquema simplificado de un sistema capaz de llevar a cabo el procedimiento de la invención.

La Fig. 2 muestra un ejemplo del contenido HTML o texto bruto de un dominio de la red oscura Tor.

La Fig.3 muestra un ejemplo del texto resultante tras el preprocesado del dominio de la red oscura Tor presentado en la Fig. 2.

La Fig. 4 muestra el Grafo de Actividades de Interés para todos los dominios ilegales de la red Tor.

La Fig. 5 muestra el Grafo de Actividades de Interés para los dominios pertenecientes a alguna de las categorías previamente mencionadas, entre ellas “contrabando de tarjetas de crédito” y “venta de drogas” de la red Tor.

La Fig. 6 muestra la salida del fichero de datos que contendría los dominios de la red oscura Tor ordenados según el valor de rango, indicando la influencia dentro de dicha red oscura.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

Se describe a continuación un ejemplo de procedimiento de acuerdo con la invención, haciendo referencia a las figuras adjuntas. La **Figura 1** muestra un esquema simplificado del sistema de rastreo, clasificación y detección de dominios más influyentes. Todo ello podría ser implementado en un ordenador 2 (que podría ser, cualquier equipo de sobremesa o portátil con un núcleo, 512MB de RAM y 8Gb de disco duro). El ordenador 2 se conecta a internet y se configura para poder acceder a la red oscura Tor 1. A continuación, se realiza un rastreo de dominios 3 y se descargan aquellos que estén activos su texto en bruto 3, obteniendo un fichero HTML de texto 4. Sobre este fichero se realiza un preprocesamiento del texto en bruto 5 para obtener el texto 6 final sobre el que se trabajará. En el ejemplo de procedimiento según la invención, se realiza también una clasificación automática del texto 6a, de la que resultan una serie de etiquetas que se corresponden con las diferentes categorías de los dominios analizados 6b. A partir del texto preprocesado 6, se realiza una extracción de los hipervínculos

entrantes y salientes de cada dominio y se construye un Grafo de Actividades de Interés 8 para toda la red oscura Tor. Adicionalmente, en este ejemplo de procedimiento según la invención, se construye un Grafo de Actividades de Interés para cada una de las categorías resultantes tras el proceso de clasificación automática. Finalmente, se aplica el algoritmo de influencia 9, dando lugar a un archivo de datos 10 donde aparecen los dominios de Tor ordenados según su valor de rango. Los dominios situados en la primera posición son considerados los más influyentes de la red. Adicionalmente, en este ejemplo de procedimiento según la invención, se genera un archivo de datos por cada una de las categorías resultantes tras el proceso de clasificación automática, donde aparecen los dominios que pertenecen a una misma categoría ordenados por su valor de rango. A continuación, se describe cada paso del procedimiento de la invención.

La conexión del ordenador 2 a internet se puede realizar a través de una conexión inalámbrica o a través de un cable de red Ethernet. La conexión del ordenador 2 a la red oscura Tor 1 comprende un proceso de instalación de un software especial que permita conectarse a dicha red oscura, como por ejemplo la instalación el navegador Tor, “Tor Browser”. El objeto de esta conexión y configuración es la obtención del texto en bruto necesario para poder realizar la clasificación automática y posterior cálculo de los dominios más influyentes.

A continuación, se procede al rastreo de dominios y descarga de texto en bruto. En primer lugar, se obtiene una lista pública de dominios de la red oscura Tor, que podría obtenerse de la Web Superficial. Dado el ciclo de vida de los dominios de la red Tor, no se facilita ningún enlace en este documento. Esta lista de dominios es leída por el programa de rastreo y se descarga el texto en bruto 3 de aquellos dominios que estén activos, obteniendo así un fichero HTML por dominio activo analizado.

La **Figura 2** muestra un ejemplo del contenido HTML o texto bruto de un dominio de la red oscura Tor. Como se puede observar, hay muchos recursos textuales no pertenecientes al lenguaje natural, como por ejemplo las etiquetas del lenguaje de programación HTML, que hay que eliminar antes de continuar con el procedimiento y así lograr una mayor precisión en la clasificación.

En la siguiente etapa se procede al preprocesamiento del texto en bruto contenido en los ficheros HTML recuperados de la red oscura Tor. Primero se eliminan las etiquetas del lenguaje HTML y, en el caso de las etiquetas que referencian imágenes, se elimina la

extensión y se deja el nombre de la imagen. A continuación, se seleccionan aquellos dominios cuyo lenguaje es el inglés, dado que es el idioma dominante de la red Tor, aunque podría realizarse con otros lenguajes. En esta realización preferente de la invención, dicha selección se realiza con la librería Langdetect (https://pypi.python.org/pypi/langdetect). Por último se eliminan caracteres especiales y palabras vacías a través de la lista de palabras vacías SMART (http://www.ai.mit.edu/projects/jmlr/papers/volume5/lewis04a/a11-smart-stop-list/). Debido al ámbito de trabajo, es decir, la red oscura Tor, se modifica dicha lista y se añaden 100 nuevas palabras para mejorar la compatibilidad. Finalmente, se unifican todos los emails, direcciones web y monedas en un único recurso textual. La **Figura 3** muestra un ejemplo del texto resultante tras el preprocesado del dominio de la red oscura Tor presentado en la **Figura 2**.

Tras el preprocesado del texto en bruto se procede a la clasificación automática de los dominios, con objeto de poder calcular cuáles son los dominios más relevantes dentro de cada categoría, y no solo identificarlos a nivel de toda la red oscura Tor. El texto ya procesado se codifica preferiblemente mediante TF-IDF (Akiko Aizawa. 2003. An information-theoretic perspective of tf–idf measures. Information Processing & Management, 39(1):45–65.), usando una longitud de vector mínima de tres y máxima de 10000 elementos. A continuación, se entrena el sistema con LR (David W. Hosmer Jr. and Stanley Lemeshow. 2004. Applied logistic regression. John Wiley & Sons), activando el balance de pesos entre clases. Las categorías resultantes son: (i) pornografía, (ii) criptomoneda, (iii) contrabando de tarjetas de crédito, (iv) venta de drogas ilegales, (v) actividades violentas, (vi) ataques cibernéticos (hacking), (vii) falsificación de moneda, (viii) contrabando de identificación personal y (ix) otros.

Una vez completado el preprocesamiento del texto en bruto y la clasificación de dominios, se construyen los Grafos de Actividades de Interés. Inicialmente se extrae para cada dominio los hipervínculos entrantes y salientes pertenecientes a los protocolos HTTP y HTTPS. Durante este proceso se eliminan los hipervínculos, y por lo tanto enlaces del grafo, duplicados, es decir, aquellos que tienen el mismo origen y destino, para evitar la creación de multigrafos, y también aquellos hipervínculos que apuntan a la Web Superficial. A continuación, se construye el Grafo de Actividades de Interés, donde los nodos se corresponden con dominios, y los enlaces con los diferentes hipervínculos entrantes y salientes contenidos en los anteriores dominios. Se genera un enlace entre dos nodos A y B siempre que el dominio A haga referencia al dominio B, o viceversa, al menos una vez.

La **Figura 4** muestra una vista general del Grafo de Actividades de Interés para todos los dominios considerados en la red Tor.

La **Figura 5** muestra una vista más detallada del Grafo de Actividades de Interés, donde se pueden ver como los nodos que representan cada dominio están categorizados y los múltiples enlaces que hay entre ellos.

Finalmente, se realiza el cálculo de la influencia de la lista de dominios para todos los dominios analizados de la red oscura Tor como para los dominios dentro de las siguientes categorías (i) pornografía 11, (ii) criptomoneda 12, (iii) contrabando de tarjetas de crédito 13, (iv) venta de drogas ilegales 14, (v) actividades violentas 15, (vi) ataques cibernéticos 16 (hacking), (vii) falsificación de moneda 17, (viii) contrabando de identificación personal 18. No se incluye la categoría otros dado que engloba actividades de múltiples tipos y ya se está calculando un listado de dominios para toda la red, con lo que se considera que no contribuye a aportar un listado relevante de dominios.

Esta medida de la influencia está basada en el cálculo del valor de rango asociado a cada dominio y la posterior ordenación descendente de dichos dominios según el valor de rango obtenido, siendo los primeros dominios los de mayor valor y, por lo tanto, los considerados como más influyentes. El algoritmo de influencia identifica el nodo más central de un grafo midiendo el número de nodos a los que puede propagar el tráfico y el número de nodos desde los que recibe tráfico. El cálculo del valor de rango consta de dos fases, una fase de inicialización y otra de actualización de pesos. Dado un Grafo de Actividades de Interés que contiene N nodos y E enlaces, el algoritmo se inicializa asignando un peso inicial I_n a cada nodo n, utilizando la siguiente fórmula:

$$W_n = D_i + D_o \qquad (1)$$

donde D_i es el valor del grado de entrada y D_o es el valor del grado de salida respectivamente. El valor D_i se relaciona con el número de enlaces entrantes de un nodo y el valor D_o representa el número de enlaces salientes de dicho nodo.

A continuación, se asigna a cada nodo n el peso acumulado de sus seguidores, que son los nodos que están apuntando al nodo n , y el peso de los nodos a los que el nodo n sigue. El valor de rango (R) se asigna al nodo n teniendo en cuenta el peso inicial W_n asignado (1)

según la siguiente fórmula:

$$R_n = W_n \log(\alpha W_F + \beta W_f) \qquad (2)$$

donde W_F es el peso acumulado de los seguidores y W_f es el peso acumulado de los nodos a los que n sigue. Los parámetros α, β controlan la contribución de los pesos de los seguidores y de los nodos a los que el nodo sigue.

El algoritmo de influencia permite identificar qué dominio es el más influyente dentro de la red, es decir, el dominio cuya eliminación provocaría la mayor desestabilización de la red. Dicha desestabilización afectaría a una reducción muy elevada u obstrucción en la transmisión de información a través de los diferentes dominios. Para medir cómo se ve afectada la transmisión de información dentro de un grafo tras eliminar un nodo, se utiliza una medida de densidad según la siguiente fórmula

$$D_G = \frac{E}{N(N-1)} \qquad (2)$$

Donde E representa el número de enlaces y N el número de nodos del grafo. Por lo tanto, una ordenación de dominios según su influencia sería aquella que tuviera la densidad más baja posible después de eliminar el menor número de nodos posibles dentro de los que hubieran obtenido una puntuación o valor de rango alta.

Una vez obtenido el valor de rango para todos los nodos, se realiza un procedimiento de evaluación donde se van eliminando del grafo uno a uno los nodos que han obtenido el mayor valor de rango y se va recalculando la densidad después de cada eliminación. Dicho proceso continua hasta que el grafo está completamente desconectado, es decir, con una densidad de 0. A través de experimentación con diferentes valores, se asigna a los parámetros los valores de 1.0 y 0.2 respectivamente como los valores finales para el algoritmo de influencia, dado que son los que permiten obtener el menor valor del área bajo la curva (AUC, “Area Under the Curve”), lo que está asociado a la densidad más baja posible a la hora de eliminar el menor número de nodos con el mayor valor de ranking.

La **Figura 6** muestra un ejemplo de la salida del fichero de datos que contendría los dominios de la red oscura Tor ordenados según el algoritmo de influencia, indicando la influencia dentro de dicha red oscura.

REIVINDICACIONES

1. Procedimiento para la clasificación y detección de los dominios más influyentes dentro de la red oscura Tor (1), caracterizado por que comprende los siguientes pasos:

- rastrear una pluralidad de dominios dentro de la red oscura Tor (1) y descargar texto en bruto (3) de al menos un dominio (7), a través de un ordenador (2) conectado a internet y configurado para acceder a la red oscura Tor (1);

- obtener un fichero HTML (4) a partir del texto en bruto (3);

- preprocesar el texto en bruto (5) para obtener un texto preprocesado (6) y una pluralidad de hipervínculos entrantes y salientes extraídos del al menos un dominio (7);

- realizar una clasificación automática (6a) del texto preprocesado (6) a través de una codificación del texto mediante vectores de características y un algoritmo de aprendizaje automático basado en regresión, y obtener una serie de categorías de dominios (6b);

- construir un grafo de actividades de interés (8) a partir de los hipervínculos entrantes y salientes extraídos del al menos un dominio (7);

- determinar el valor de rango (9) para cada dominio, que se obtiene como la combinación ponderada de la suma del número de enlaces de cada nodo, obtenidos los enlaces a partir de los hipervínculos a dominios seguidores y seguidos de cada dominio (7);

- realizar una ordenación de los nodos, y por lo tanto de los dominios correspondientes, según su valor de rango;

- etiquetar los dominios con mayor valor de rango como aquellos más influyentes dentro de la red oscura Tor.

2. Procedimiento según la reivindicación 1, donde el preprocesamiento del texto en bruto (5) de los ficheros HTML (4) comprende:

- eliminar las etiquetas del lenguaje HTML;

- eliminar extensión y dejar el nombre de la imagen en el caso de las etiquetas que referencian imágenes;

- seleccionar los dominios en inglés con una librería de detección de idioma;

- eliminar caracteres especiales y palabras vacías a través de una lista de palabras vacías;

- editar y añadir una pluralidad de nuevas palabras vacías para mejorar la compatibilidad con el dominio de la red oscura Tor;

- unificar todos los emails, direcciones web y monedas en un único recurso textual.

3. Procedimiento según la reivindicación 1, donde el paso de realizar una clasificación automática de los dominios (6a) comprende:

- codificar el texto ya procesado mediante la técnica de Frecuencia de Términos – Frecuencia Inversa del Documento usando una longitud de vector de características de entre tres y 10000 elementos;

- entrenar un algoritmo de aprendizaje automático con un conjunto de entrenamiento etiquetado utilizando Regresión Logística, y activando el balance de pesos entre clases;

- clasificar, utilizando el algoritmo de aprendizaje automático entrenado, los dominios de la red oscura Tor (1) en al menos una de las nueve clases definidas:

  - pornografía,
  - criptomoneda,
  - contrabando de tarjetas de crédito,
  - venta de drogas ilegales,
  - actividades violentas,
  - ataques cibernéticos,
  - falsificación de moneda,
  - contrabando de identificación personal, y
  - otros.

4. Procedimiento según la reivindicación 1, que comprende mostrar una etiqueta de cada bloque de texto (6) una vez ha sido clasificado.

5. Procedimiento según la reivindicación 1, que comprende la construcción de un grafo de actividades de interés (8) para toda la red oscura Tor (1) y un grafo de actividades de interés (8) por cada categoría resultante de la clasificación (6b) a través de los hipervínculos entrantes y salientes (7) de cada dominio, donde la construcción del grafo de actividades de interés comprende:

- extraer para cada dominio los hipervínculos entrantes y salientes pertenecientes a los protocolos HTTP y HTTPS;

- eliminar los hipervínculos que tienen el mismo origen y destino, y los hipervínculos que apuntan a la Web Superficial;

- construir un Grafo de Actividades de Interés, donde los nodos se corresponden con dominios, y los enlaces con los diferentes hipervínculos entrantes y salientes contenidos en los anteriores dominios de forma que se genera un enlace entre dos

nodos A y B siempre que el dominio A haga referencia al dominio B, o viceversa, al menos una vez.

6. Procedimiento según la reivindicación 1, que comprende el cálculo del algoritmo de influencia para todos los dominios del Grafo de Actividades de Interés global (8), identificándose como dominios más relevantes dentro de la red oscura Tor aquellos que obtienen los mayores valores de rango, donde el cálculo del valor de rango para un dominio cualquiera comprende:

- inicializar el valor de rango con un peso inicial basado en el número de enlaces entrantes y salientes de dicho nodo dentro del Grafo de Actividades de Interés;
- actualizar el valor de rango teniendo en cuenta el peso inicial y la suma ponderada del peso acumulado de sus dominios seguidores y seguidos, donde la influencia de los pesos de los dominios seguidores y seguidos se calcula a través de dos parámetros α, β.

7. Procedimiento según la reivindicación 1, que comprende el cálculo del algoritmo de influencia para todos los dominios del Grafo de Actividades de Interés global (8) calculado para cada categoría, identificándose como dominios más relevantes dentro de cada categoría de la red oscura Tor aquellos que obtienen los mayores valores de rango dentro de la categoría seleccionada, donde el cálculo del valor de rango para un dominio cualquiera comprende:

- inicializar el valor de rango con un peso inicial basado en el grado de entrada y salida de dicho nodo, es decir, el número de enlaces entrantes y salientes de dicho nodo dentro del Grafo de Actividades de Interés;
- actualizar el valor de rango teniendo en cuenta el peso inicial y la suma ponderada del peso acumulado de sus dominios seguidores y seguidos. La influencia de los pesos de los dominios seguidores y seguidos se calcula a través de dos parámetros α, β.

8. Sistema para la clasificación y detección de los dominios más influyentes dentro de la red oscura Tor caracterizado por que comprende medios de procesamiento de datos (2) configurados para:

- rastrear una pluralidad de dominios dentro de la red oscura Tor (1) y descargar texto en bruto (3) de al menos un dominio (7), a través de un ordenador (2) conectado a internet y configurado para acceder a la red oscura Tor (1);
- obtener un fichero HTML (4) a partir del texto en bruto (3);

- preprocesar el texto en bruto (5) para obtener un texto preprocesado (6) y una pluralidad de hipervínculos entrantes y salientes extraídos del al menos un dominio (7);

- realizar una clasificación automática (6a) del texto preprocesado (6) a través de una codificación del texto mediante vectores de características y un algoritmo de aprendizaje automático basado en regresión, y obtener una serie de categorías de dominios (6b);

- construir un grafo de actividades de interés (8) a partir de los hipervínculos entrantes y salientes extraídos del al menos un dominio (7);

- determinar el valor de rango (9) para cada dominio, que se obtiene como la combinación ponderada de la suma del número de enlaces de cada nodo, obtenidos los enlaces a partir de los hipervínculos a dominios seguidores y seguidos de cada dominio (7);

- realizar una ordenación de los nodos, y por lo tanto de los dominios correspondientes, según su valor de rango;

- etiquetar los dominios con mayor valor de rango como aquellos más influyentes dentro de la red oscura Tor.

9. Sistema según la reivindicación 8, que comprende un ordenador (2) conectado a internet y configurado para poder acceder a la red oscura Tor (1), conteniendo el programa para el rastreo y descarga de texto en bruto (3), el programa para la clasificación automática de texto (6a), la construcción del Grafo de Actividades de Interés (8), el cálculo del valor de rango para todos los dominios analizados y la indicación sobre los dominios más relevantes de la red oscura Tor (10) a nivel global y por categorías.

10. Sistema según cualquiera de las reivindicaciones 8 a 9, que comprende unos medios de almacenamiento de datos donde se almacenan los archivos HTML (4), el texto preprocesado (6), las categorías de los dominios analizados (6b) y el archivo de datos con las listas de dominios ordenados según su nivel de influencia.

11. Un producto de programa que comprende medios de instrucciones de programa para llevar a cabo el procedimiento definido en cualquiera de las reivindicaciones 1 a 7 cuando el programa se ejecuta en un procesador.

12. Un producto de programa según la reivindicación 11, almacenado en un medio de soporte de programas.

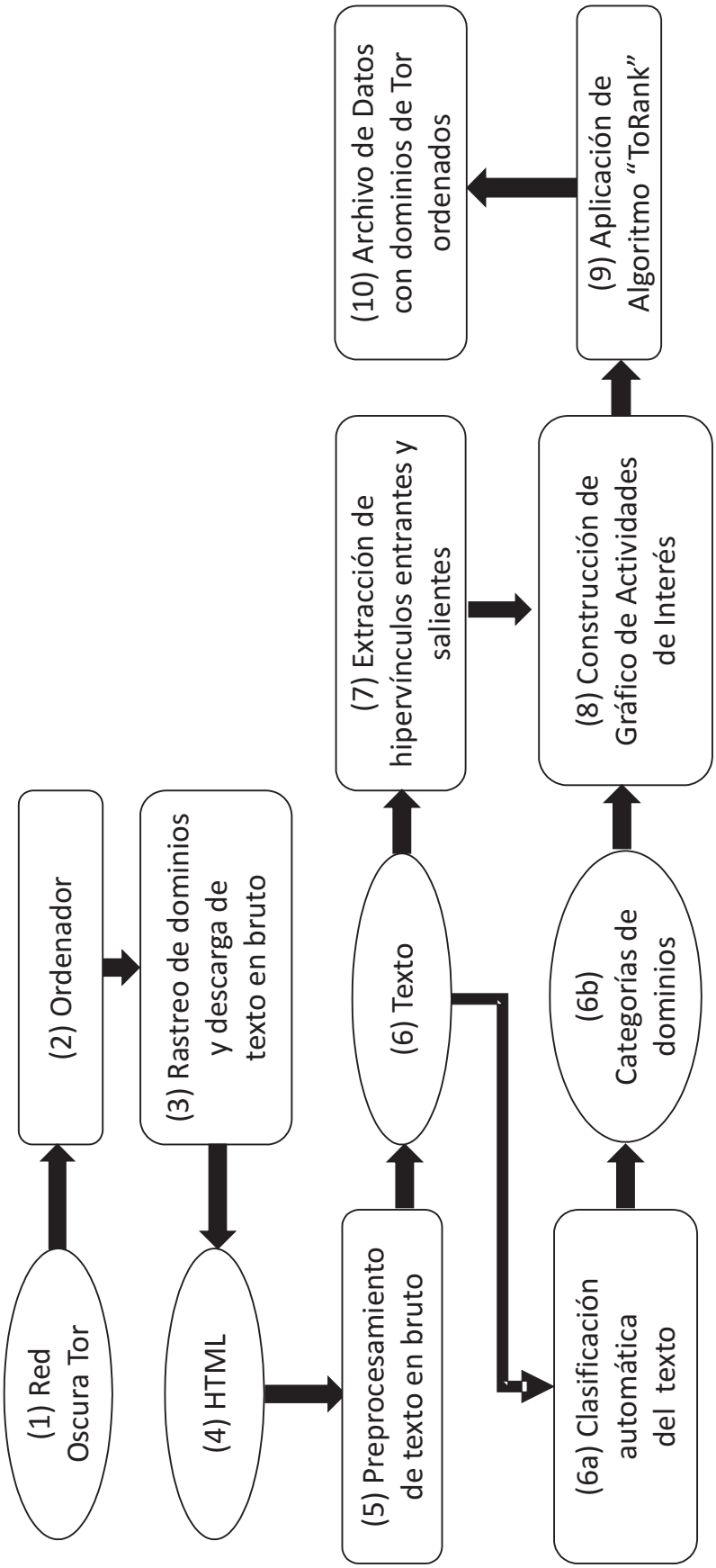
(1) Red Oscura Tor
(2) Ordenador
(3) Rastreo de dominios y descarga de texto en bruto
(4) HTML
(5) Preprocesamiento de texto en bruto
(6) Texto
(6a) Clasificación automática del texto
(6b) Categorías de dominios
(7) Extracción de hipervínculos entrantes y salientes
(8) Construcción de Gráfico de Actividades de Interés
(9) Aplicación de Algoritmo "ToRank"
(10) Archivo de Datos con dominios de Tor ordenados

Fig. 1

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">

<head>
  <title>TDS</title>
  <meta name="description" content="The Drug Store" />
  <meta name="keywords" content="Drugs" />
  <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  <link rel="stylesheet" type="text/css" href="http://x2u26l2gxxxkrbrz.onion/css/style.css" />
  <script type="text/javascript" src="http://x2u26l2gxxxkrbrz.onion/js/jquery.min.js"></script>
  <script type="text/javascript" src="http://x2u26l2gxxxkrbrz.onion/js/jquery.easing.min.js"></script>
  <script type="text/javascript" src="http://x2u26l2gxxxkrbrz.onion/js/jquery.nivo.slider.pack.js"></script>
  <script type="text/javascript">
    $(window).load(function() {
        $('#slider').nivoSlider();
    });
  </script>
</head>

<body>
  <div id="main">

    <div id="menubar">
      <div id="welcome">
        <h1><a href="contact.html#">The Drug Store</a></h1>
      </div><!--close welcome-->
      <div id="menu_items">
        <ul id="menu">
          <li><a href="index.html">Home</a></li>
          <li><a href="ourmission.html">Our Mission</a></li>
          <li><a href="faq.html">F.A.Q.</a></li>
          <li><a href="projects.html">Projects</a></li>
          <li class="current"><a href="contact.html">Contact Us</a></li>
        </ul>
      </div><!--close menu-->
    </div><!--close menubar-->
```

Fig. 2

```
drug store mission project start drug question visit section updat updat vendor order send email bitmessag copi fill past text
drug amount weight region ship note prefer vendor prefer market shortli bang buck satisfi simpli complet order mail forward ser
vic ident vendor hand strongli suggest mail forward servic ident hand email <email> bitmessag offer multisig default transact m
ultisig read news vendor verif applic cancer awar support drug store frequent question market multipl safeti peer review anonym
mail forward servic deal vendor event vendor marketplac compromis mail inform secur multisig transact marketplac impliment trus
t vendor rate pre screen vendor minimum requir order verifi vendor item verifi undeliv track show undeliv order reship question
vendor offer kool aid fund nicer faster alot vendor charg fee live total transact donat cover oper cost mail forward server gra
pe kool aid site seiz extrem length mitig issu seizur law enforc thing case outag due forc immedietli announc url offici bitmes
sag anonym mail forward servic simpli put accept packag behalf reship address suggest due profession courtesi <url> friend smar
t read review payment method accept love bitcoin litecoin darkcoin dogecoin law enforc dont law enforc encourag anonym mail for
ward servic deal doubt grape kool aid understand addict drug store mission clear simpl elimin hassl worri drug market make purc
has liter drug extrem easi fast drug store work trust vendor product stock readi ship multipl market longer scroll endlessli pr
oduct find reliabl vendor pre screen work relationship major top vendor ensur qualiti stabil reship item verifi undeliv questio
n period accept major crypto currenc exchang privaci mission read project work hard improv infrastructur supplier list happi an
nounc abil stock larg quantiti hand select item news dedic idea move drug trade shadi danger real world trade commonli bundl in
ferior qualiti drug market vital step accomplish task flaw process goal mitig flaw end end servic reward honest vendor end cons
um remain safe anonym reciev qualiti imagin accept major crypto currenc privaci offer anonym mail forward servic default vendor
address case market vendor seizur encourag peer review mail forward servic extrem strict custom polici safe real address due co
nstant updat fluctuat product list price work simpl platform work shift 7 clock includ holiday simpli put stop work vendor mark
et verifi list find quot price specif vendor prefer happi accommod drug store make life easi guarante simplest safest drug buy
experi turn charg flat fee cover oper cost grape kool aid addict joke good practic privat transpar answer question servic minu
opsec idea commun open arm good idea improv buy experi increas secur readi part transact multisig default rip love td learn mul
tisig protect feedback suggest vendor applic open accept applic verifi vendor requir publicli verifi vendor major market equivi
l higher feedback vendor older market drug miltisig cancer awar support drug store
```

Fig. 3

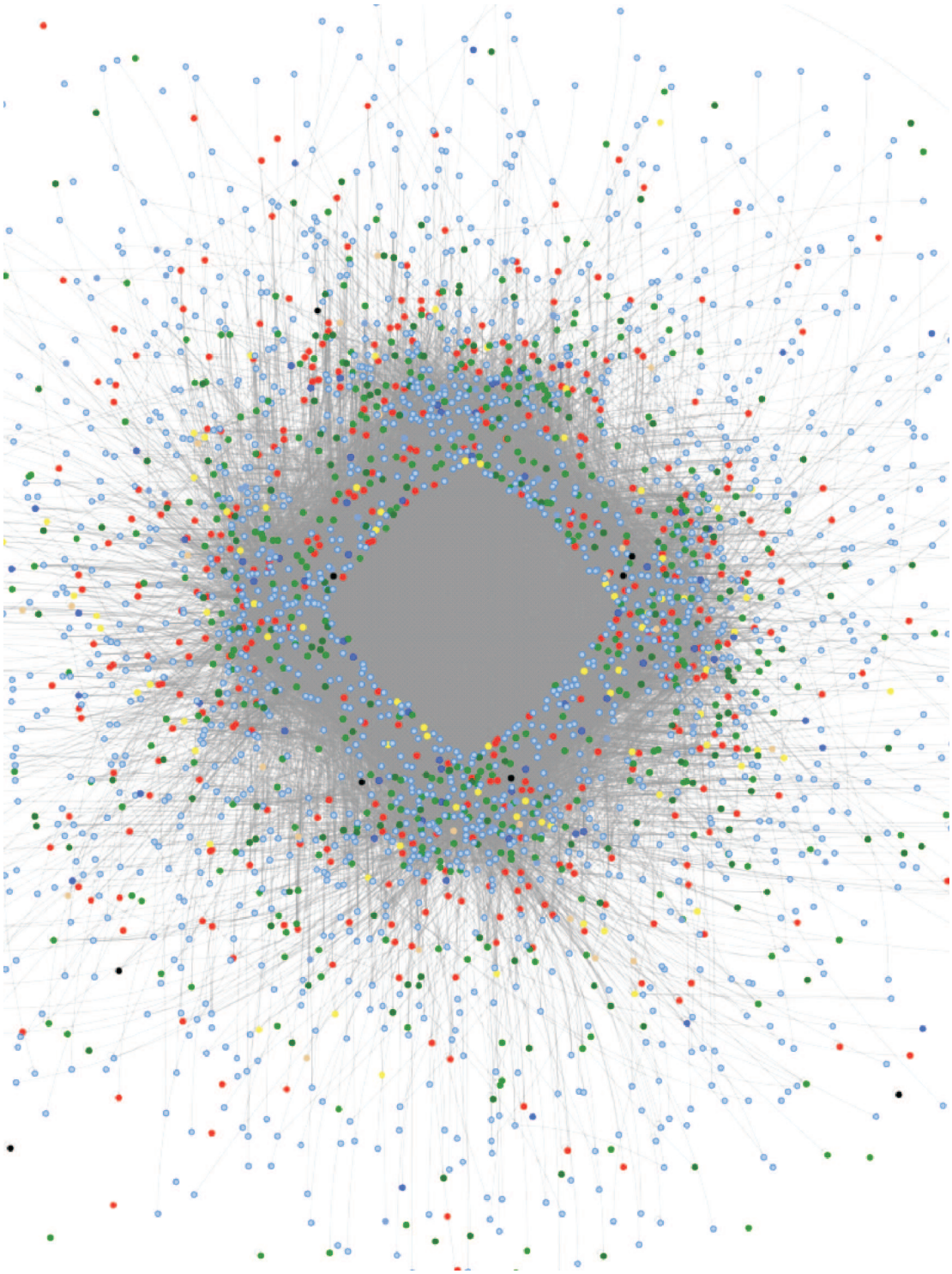

Fig. 4

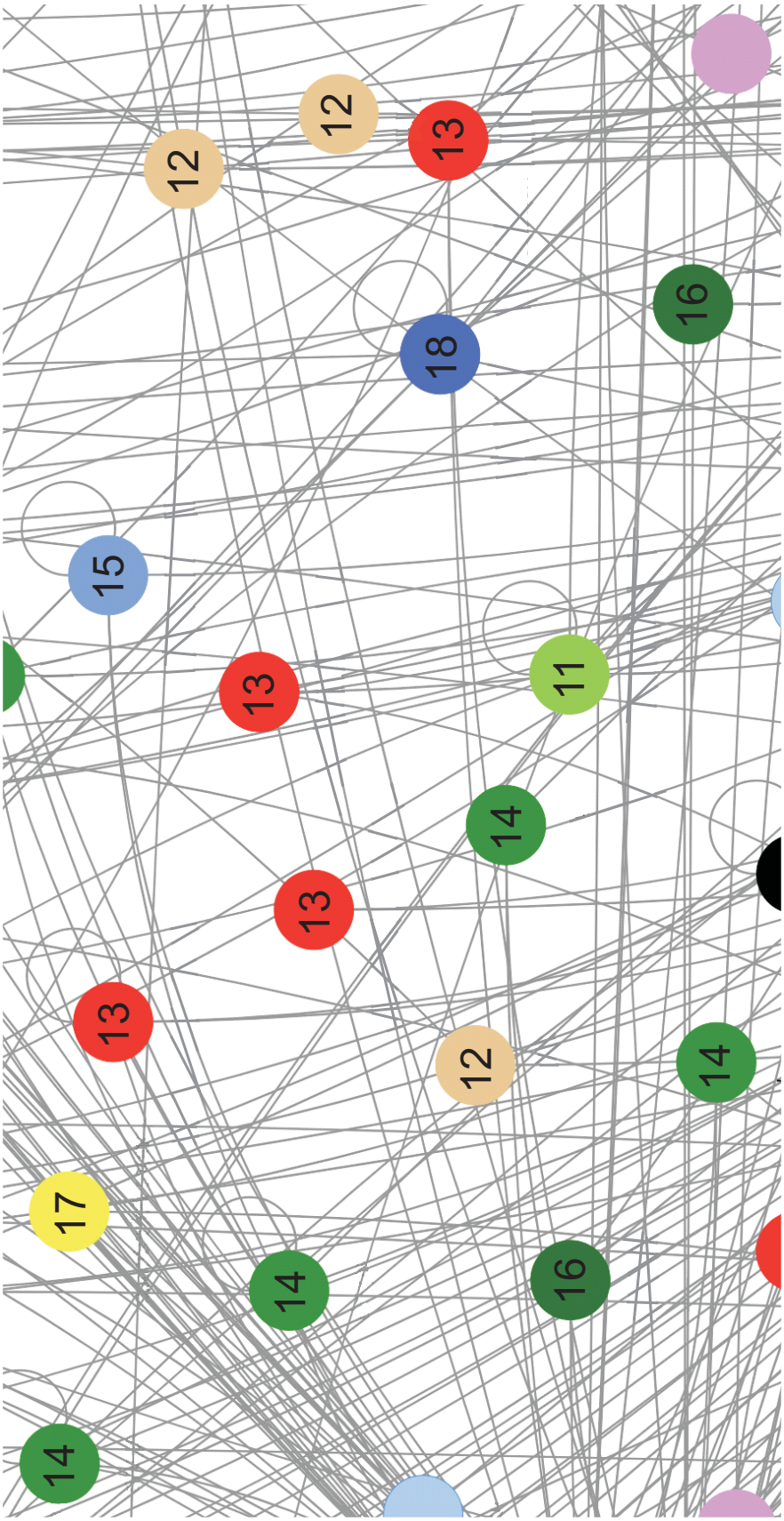

Fig. 5

Ranking	Dominio	Categoría
1	rsci7rl3rmpcsvyf.onion	Violence
2	doxtorg7natnwyz5.onion	Violence
3	luckp47s6xhz26rn.onion	Violence
4	vandyrjcpk3pw5ne.onion	Violence
5	mke3j4vlpo3ccmu4.onion	Hosting/ Server
6	weapon5cd6o72mny.onion	Violence
7	yy4jga5rhw2qupdk.onion	Violence
8	gunsammoaahtpmqs.onion	Violence
9	sm66ogcqy3vastv3.onion	Personal
10	gunsay5oixhyvj64.onion	Violence

Fig. 6