Deep Web

El monstruo de la red

Deep Web

El monstruo de la red

Facundo David Gallo

Ra-Ma®

La ley prohíbe
fotocopiar este libro

Editado por:
RA-MA Editorial
Calle Jarama, 3A, Polígono Industrial Igarsa
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: *editorial@ra-ma.com*
Internet: *www.ra-ma.es* y *www.ra-ma.com*
ISBN: 978-84-1855-111-6
Depósito legal: M-29071-2020
Maquetación: Antonio García Tomé
Ilustración de portada: Haxadarkart
Filmación e impresión: Safekat
Impreso en España en diciembre de 2020

A mi familia por permitirme la ventaja de escribir
a largas horas de la noche,
incluso cuando se torna difícil compaginarlo
con las obligaciones personales.

A "M", perteneciente al cuerpo de la Policía Nacional,
por sus consejos medidos sobre cierta información
que por seguridad no ha sido publicada en la presente obra.

A los investigadores que descendieron en busca de su propio Kraken
y no hallaron más que el desasosiego o la rendición.
Que la presente obra sirva como motor de impulso
para nunca rendirse ante lo improbable.

ÍNDICE

SOBRE EL AUTOR

Como buscador incansable y pirata informático de los que no se ocultan para poder subsistir, decidí incursionar en la convergencia de la ciberseguridad y el mundo de la criminología dando como resultado el presente libro.

Doctorando en cibercrimen, con un Grado universitario en ingeniería informática, un Máster universitario en ciberseguridad y un Máster universitario en divulgación científica, me he tomado la licencia de arropar la obra bajo alguna que otra pincelada técnica gracias a los primeros estudios, mientras que la comunicación me ha permitido aplicar algo de didáctica a términos que suelen ser complejos de trasladar.

Trabajo desde los 18 años en el sector de la informática, aún no he bajado la guardia y me queda mucha gasolina que quemar.

Facundo D. Gallo

PRÓLOGO

Entre las paradojas de estos tiempos de incertidumbre se encuentran el progresivo sacrificio de la privacidad en aras de una, hipotética, mayor seguridad y, sobre todo, una inconsciente y generalizada devaluación del anonimato. Mientras Estados y organizaciones, con sus correspondientes instituciones y agencias, comités y defensores del ciudadano, se empeñan en defender la privacidad y proteger los datos personales, son muchas las personas que asisten apáticas e indiferentes, incluso contrariadas, a este complejo montaje de normas, órganos, requisitos y consentimientos que no quieren o no pueden entender. No es difícil tener la impresión de que los gobernantes están caminando en dirección contraria al sentir de los ciudadanos para quienes la idea de privacidad y el valor del anonimato no necesariamente tienen el mismo significado. Por otra parte, sin embargo, esos mismos Estados y organizaciones, con sus correspondientes instituciones y agencias, están embarcados en el debate sobre la encriptación alegando motivos de seguridad ciudadana o nacional para justificar el acceso a los datos personales y al ámbito de la privacidad que, con tanta insistencia y medios, por otra parte, aseguraban querer defender.

En la sociedad de la vigilancia, el anonimato, ese bien tan preciado y cada vez más escaso, es el fundamento y la razón de ser de la Deep Web donde no hay seguridad, ni parece posible aplicar la legalidad: un alto precio a pagar. Entre la utopía de un mundo sin vigilancia y la distopía de un mundo sin reglas, la Deep Web sigue siendo un mundo desconocido para la gran mayoría. Con esa obra Facundo David Gallo ofrece al lector la posibilidad de entender ese mundo bipolar.

Esta monografía se estructura en cinco capítulos que responden a una atractiva, a la par que didáctica y dinámica, organización secuencial. Tras un primer capítulo introductorio, la división zonal de las superficies del mar obra el milagro

–por mérito del autor– de adentrarnos de un modo prácticamente visual, pero realmente conceptual, en el proceloso mundo de la Deep Web.

El primer capítulo, bajo el ilustrativo título "Curso rápido de buceo", ofrece una panorámica precisa del objeto de esta monografía prodigando información y conocimientos sobre la filosofía de las profundidades –en las que se cruza el umbral hacia lo desconocido y se entra en el imperio del anonimato–, las medidas de compresión para el buceo –que permiten ese anonimato– y los medios alternativos de exploración como la Freenet o el Invisible Internet Project (I2P).

Tras esta explicación introductoria, el lector agradecerá la advertencia con la termina el capítulo I y comprenderá su significado al completo, incluido el agradecimiento a las fuerzas y cuerpos de seguridad del Estado, al final del inquietante trayecto que proponen sus páginas. No hay que olvidar, como advierte el autor, que la filosofía de la red Tor "se basa en asegurar el anonimato de los usuarios, haciéndolo incompatible con los controles y estándares de seguridad que garantizan las trazabilidades o registros de usuarios, de tal manera que resulta complejo aplicar medidas de restricción legal sobre los contenidos publicados".

A partir de ahí, los capítulos II a V se explican como un tránsito desde las zonas Fótica a Batial, Abisal y, finalmente, Hadal en una exploración que permite, en una progresión creciente en este avance metafórico, pero no por ello menos inquietante, hacia esas profundidades, conocer y comprender el significado, el entramado y el funcionamiento de esta suerte de submundos que constituye la Deep Web.

En el capítulo II, dedicado a la llamada Zona Fótica (0 a 1.000 ms. de profundidad), próxima a la Surface Web que conocemos, el autor explica la tecnología P2P, el archivo Torrent y el Protocolo BitTorrent que opera mediante un modelo de funcionamiento distribuido basado en fragmentar el fichero destino entre varios hosts y con un nodo generador principal denominado semilla. La filosofía que subyace detrás de esta metodología consiste en situar a cada nuevo usuario como punto de distribución. Sobre esa base conceptual, se analizan, ilustrando con imágenes y tablas, los casos de la Mazmorra de lo Grotesco, Sad Satan, el complejo entramado de símbolos del misterio "432" y sus significados y la Fundación Cryptome, un extenso archivo de supuestas filtraciones que parecen involucrar a los gobiernos estadounidense y británico.

El capítulo III se ocupa de la Zona Batial (1.000 a 4.000 ms. de profundidad), definido como el hábitat de una escasa fauna que nada libremente pero que nunca se aproxima a la superficie y en la que sus habitantes deben recurrir al único alimento existente: la depredación de otros organismos. Este capítulo se subdivide en un

primer apartado sobre "Como guiarse en la oscuridad" y uno segundo denominado "comunicaciones a ninguna parte".

El primero se construye buscando referentes conforme al modelo de la Surface Web para guiarnos sobre algunos de sus contenidos. El autor identifica y explica el tipo de buscadores como Torch, AHMIA y DarkSearch, que presentan ventajas e inconvenientes. Hidden Wiki cumple funciones similares, salvando las distancias, a las de una Wikipedia. Los sistemas de hosting y para la creación de webs siguen una lógica también similar en la medida en que pueden contratarse a terceros o crearse por el usuario mismo, si se tienen los conocimientos necesarios a esos efectos. Imágenes y tablas informan sobre condiciones y precios con la particularidad de que no hay límites en cuanto al uso, pero tampoco garantías de que, efectivamente, se vaya a cumplir con el servicio contratado y pagado por adelantado. El dilema libertad *versus* seguridad se manifiesta de un modo tan extremo que incluso le hace perder su significado. Siguiendo con las referencias conocidas, las cuentas de correo funcionan con una lógica parecida a las conocidas en la Surface Web.

En cambio, las denominadas "Comunicaciones a ninguna parte" se sitúan en un territorio algo diferente. Aunque responden a las mismas necesidades de la Surface Web, las dinámicas son distintas: confesionarios donde se confiesa lo que sería inconfesable; chats donde se habla de lo que no debería verbalizarse; y foros, como OnionChan, que funciona como un Guadiana con intervalos activos e inactivos y contenidos consistentes, básicamente, en la circulación de material ilícito, que el autor ilustra con imagen y datos.

El capítulo IV lleva al lector a la Zona Abisal (4.000 a 6.000 ms. de profundidad) donde el autor le recibe explicando el significado del término abismo: un lugar profundo y frío por la ausencia total de luz habitado por animales con apariencia monstruosa y movido por dinámicas vitales alejadas de todo sentido común. Es la Dark Net.

En una breve introducción, bajo el título "Sin sentidos", se advierte sobre la irracionalidad de los contenidos y sobre la forma en la que el autor aborda su análisis que se articula en una parte dedicada a los denominados objetos hundidos y otra sobre la llamada fauna más salvaje. Drogas, armas, tarjetas de crédito, pasaportes o herramientas cibernéticas maliciosas entran en la primera categoría y se explican con una profusión de imágenes y datos que permiten calibrar el alcance y la naturaleza de este mercado. Asesinos a sueldo, que se publican abiertamente en esta red, y piratas informáticos, que trabajan al otro lado de la legalidad, protagonizan ese escenario dentro de la fauna más salvaje.

El capítulo V corresponde a la Zona Hadal (6.000 a 11.000 ms. de profundidad) que significa lugar de muerte. Leyendas y mitos, como el del ejército fantasma,

coexisten en este espacio con una realidad en la hay dominios independientes –".loki" o ".clos"– o portales como "liberté". Una atención especial dedica el autor a la denominada leyenda del Kraken de la Deep Web: la RedRoom o DarkRoom donde supuestamente se practica el asesinato en directo. Imágenes de capturas de pantalla, datos y tablas cuidadosamente explicadas por el autor consiguen transportar al lector al núcleo duro de la zona Hadal.

Este recorrido experto por la Deep Web es posible gracias a la maestría profesional, técnica y expositiva de Facundo David Gallo. Responsable actualmente de la oficina de ciberseguridad, CISO, de la Empresa Castroalonso y con amplia formación académica en distintos centros nacionales y extranjeros, Facundo David Gallo ha trabajado como consultor de ciberseguridad, seguridad informática y gobierno de la seguridad en distintas empresas y en instituciones públicas y también como profesor, en una larga trayectoria de compromiso personal y profesional con la ciberseguridad. Solo la combinación de una grandísima experiencia y unos sólidos conocimientos con una definida vocación y un compromiso personal con la ciberseguridad puede explicar la entidad y el valor del trabajo realizado con esta inmersión en los mundos subterráneos de la Deep Web. A su Grado universitario en Ingeniería Informática, el autor suma un Máster Universitario en Ciberseguridad y un Máster en Divulgación científica, creando el entramado perfecto para escribir una obra científicamente sólida, técnicamente impecable y comprensible para cualquiera que quiera acercarse al conocimiento de la Deep Web. Con mi enhorabuena por el trabajo va también mi agradecimiento por haberme permitido el honor de prologar esta extraordinaria monografía.

INTRODUCCIÓN

La presente obra de carácter divulgativo es el fruto de una investigación llevada a cabo entre los años 2015 y 2020 sobre el amplio mundo de mitos y hechos contrastables que subyacen tras la red de anonimato más conocido del mundo, la "Deep Web" y otros medios de difusión; explorando desde los casos más cercanos y digeribles sobre la difusión de información confidencial, pasando el mercado negro en todas sus vertientes, hasta los rincones donde se hallan los verdaderos horrores.

Es un objetivo primero asegurar la completa inmersión a la realidad alternativa de Internet siempre desde la experiencia propia del autor y procurando esquivar, dentro de lo posible, todo detalle técnico para así dejar un testimonio al público general.

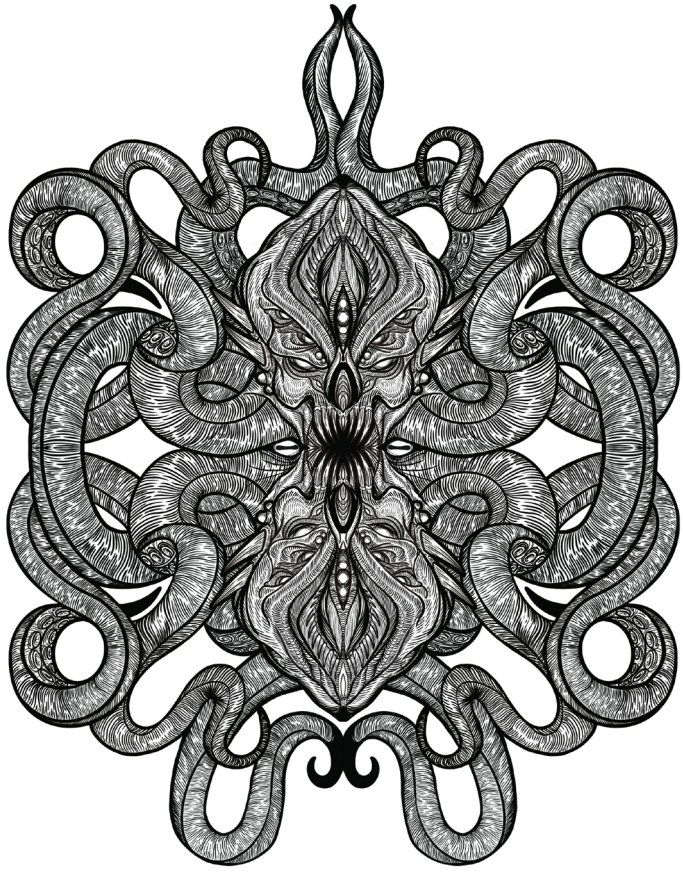
Aunque muchos hayan oído hablar del término "Deep Web" y otros aún desconozcan por completo su significado, la realidad es que nunca deja indiferente a nadie. La cara oculta de la gran red de redes sigue atrapando a todo aquel que se adentra en su basto alcance donde los límites divisorios entre legalidad e ilegalidad son inexistentes.

En la redacción de este libro he utilizado de manera recurrente términos como navegar y bucear, conocidos y utilizados por todos, para describir como nos movemos por la red; de igual forma he querido dotar de "materia" a ese lado oscuro de Internet y para ello he utilizado una figura retórica de un ser mitológico:

EL KRAKEN

El Kraken es una enorme y colosal criatura marina de la mitología escandinava descrita comúnmente como un pulpo o calamar gigante que, emergiendo de las profundidades, ataca barcos y devora a los marineros. Kraken proviene de la palabra escandinava krake que designa un animal enfermizo y algo retorcido, adjetivos que también pueden aplicarse a la Deep Web.

A este ser me he permitido incorporarle el termino *2.0* ya que el internauta tiene la posibilidad de interactuar con el resto de los usuarios o aportar contenido a la Deep Web. De esta fusión ha surgido:



Kraken 2.0

Equípese con su mejor escafandra y únase a esta cuenta regresiva para sumergirse en la apasionante búsqueda del Kraken 2.0.

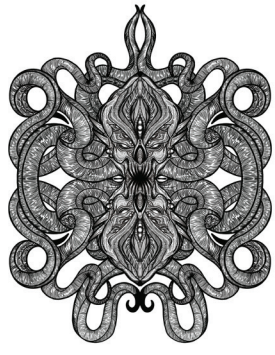
1

CURSO RÁPIDO DE BUCEO POR LA DEEP WEB

En la era de la revolución informática existe una gran ventana que con el paso de los años se ha ido consolidado por cristales de múltiples tinturas; podemos detenernos ante la imponente cristalera y recopilar solo aquellos fragmentos pertenecientes a la gama de colores cálidos, fieles representantes de la armonía, la verdad y la templanza, pero también podemos caer en la atracción por los colores fríos y entonces el discurso cambiar radicalmente. Esta gran ventana es lo que conocemos como Internet, una fuerza arrolladora que no ha parado de crecer desde el latir de sus orígenes militares hasta generar la dependencia que hemos abrazado como sociedad digital.

Otra imagen más clásica sobre el concepto Internet la podemos proyectar si imaginamos este universo de unos y ceros como la biblioteca más grande de la historia de la humanidad, y es que no resulta desatino admitir que se trata del principal punto de encuentro para diversas corrientes de pensamiento.

Si las habladurías no son tales, y resulta que hasta el Vaticano guarda un libro por cada obra lanzada al fuego inquisidor; ¿dónde se encuentran entonces los datos no convencionales de Internet?, ¿cómo podemos acceder a la gama de colores fríos?



1.1 APRECIACIÓN DESDE LAS ORILLAS

Para responder a las anteriores inquietudes necesitaremos acceder a un entramado de frías corrientes marinas y despojarnos de todo pensamiento racional y moral, porque navegar en las profundidades es trasgredir el umbral hacia lo desconocido. Cuando nos adentramos hacia un Internet ajeno a los métodos de navegación convencionales accederemos al lado oculto de la gran red de la información y a esta área restringida e invisible la denominamos Deep Web (en adelante DW), siendo su antónimo Surface Web (en adelante SW).

Todos tenemos claro que para evitar el control de las fuerzas de seguridad debemos escondernos lo mejor posible, y esta es una lección que conocen muy bien aquellos que se mueven fuera de los límites de la legalidad. La DW funciona como un reloj gracias a esta misma estrategia, pues gran parte de su filosofía se sustenta en la capacidad de ofrecer el "completo" anonimato de sus usuarios para proteger la identidad de quienes la frecuentan, y todo mediante un mecanismo denominado Tor (acrónimo de The Onion Router).

Aún recuerdo cuando el buceo mediante redes anónimas se antojaba accesible a unos pocos iniciados, y es que a principios del siglo XXI uno oía hablar de redes Tor con esa extraña sensación entre incredulidad y fascinación; no debemos olvidar que por aquel entonces el proyecto se encontraba en manos del Laboratorio de Investigación Naval de los Estados Unidos [1] ergo resulta comprensible que a este servidor, con tan solo quince años de edad, se le iluminasen los ojos cada vez que oía hablar de un hacker oculto tras las redes Tor; en lo personal recuerdo aquellos días como una sensación equiparable a tener constancia sobre la prueba definitiva de vida extraterrestre pero sin poder corroborarlo; uno sabía que existía, pero desconocía cómo ser testigo del milagro.

No fue hasta que Tor cayó en manos de la organización The Tor Project, Inc [2] cuando se expandió el uso liberado de la red, facilitando de manera significativa las herramientas para acceder a la DW.

1 Pandasecurity. Tor y deepweb todos los secretos. Recuperado de: https://www.pandasecurity.com/spain/mediacenter/seguridad/tor-y-deepweb-todos-los-secretos/

2 Torproject. History. https://www.torproject.org/about/history/

1.2 FILOSOFÍA DE LA RED TOR

No olvidemos nunca que la filosofía de la red Tor se basa en asegurar el anonimato de los usuarios, haciéndolo incompatible con los controles y estándares de seguridad que garantizan las trazabilidades o registros de usuarios, de tal manera que resulta complejo aplicar medidas de restricción legal sobre los contenidos publicados. Por consiguiente, no se antoja difícil encontrar material que va desde un documento gubernamental, supuestamente clasificado, hasta dantescas escenas de videos de tortura, violación y muerte; como bien se adelantaba en el prólogo, una de las misiones de este libro es mostrar al ciudadano lo sencillo que puede llegar a ser el acceso a este contenido separando en todo momento, y con total transparencia, los mitos de las realidades.

Un compendio de datos recabados por la Encyclopedia Britannica [3] exponen que para el año 2001, la DW pudo haber alcanzado la cifra de 7.5 petabytes de información y esto a día de hoy sigue representando una cantidad descomunal de datos; por otro lado, y lejos de las aproximaciones estadísticas, si nos preguntamos sobre la verdadera extensión de este submundo de Internet debemos hacer un ejercicio de humildad y reconocer que no puede cuantificarse empíricamente, entre otras cosas porque muchos datos son intermitentes y la información que ahora mismo está disponible puede que desaparezca en un par de minutos; tirar la piedra y esconder la mano casi siempre funciona para evitar una multa.

Otro dato a tener en cuenta para conocer la complejidad de cuantificación es la escasa indexación de contenido. La indexación es un término informático que versa sobre la posibilidad de listar en buscadores las páginas webs disponibles en Internet, estos buscadores funcionan como una guía telefónica que, en lugar de contener nombres y direcciones de personas físicas, recoge nombres y direcciones hacia portales webs. En este sentido existen motores de búsqueda que nos pueden ilustrar y que todos conocemos sea por noticias o por uso propio; es el caso de los gigantes tecnológicos Google [4]o Bing[5], por citar los más utilizados.

Ahora que somos capaces de visualizar el concepto de indexado, es importante señalar que no se aplica la misma lógica en la DW; si bien ha crecido la integración de buscadores como veremos más adelante, apenas se indexa una mínima parte del volumen total de los portales, esto nos complica la labor de búsqueda hasta llegar al

3 Pierluigi Paganini. The Deep Web: The Internet's Dark Side. Recuperado de: https://www.britannica.com/topic/Deep-Web-The-Internets-Dark-Side-The-2010684

4 Google. Google.com

5 Bing. Bing.com

contenido deseado porque aquí entra en juego otra clave dentro de la filosofía de la DW: enlaces hacia contenidos que se mantienen en secreto y se distribuyen con el boca a boca.

Recapitulemos por un momento. Se habló que la DW, entre otras características, almacena contenidos efímeros difíciles de localizar y naturalmente te preguntarás ¿Qué ocurre si hago una batería de intentos escribiendo en mi navegador de Tor algo así como "#.com"? siendo # el tipo de contenido que quiero encontrar.

En efecto, podríamos intentarlo en un navegador que funcione para SW y existiría alguna probabilidad de encontrar una página web relacionada, pero en la DW esta técnica no serviría de mucho ya que no funciona con dominios al uso ni tampoco con nomenclaturas intuitivas.

Para entender mejor el concepto de dominios vamos a imaginar que estamos en nuestra casa y necesitamos indicar a otra persona cómo enviarnos un paquete por correo ordinario

¿Qué tipo de información le proporcionaríamos?

La dirección y nuestro nombre conforman el conjunto de datos esenciales para el éxito de la entrega, porque nos identifica inequívocamente más allá del propio DNI o pasaporte que en este caso no aplicaría.

En esencia, un dominio funciona como una dirección física que nos permite encaminar el correo (petición web) al destino exacto (página web), y está formado por la siguiente nomenclatura:

"Nombre+Extensión"

Y para ejemplificarlo, que mejor que recurrir nuevamente al dominio más famoso, "google.com", donde "google" representa el nombre del dominio y ".com" la extensión.

Cuando nos referíamos a que la búsqueda aleatoria de términos en el navegador de Tor no resulta una práctica viable, es precisamente porque en la DW los nombres de dominios están formados por 16 caracteres alfanuméricos generados manualmente, representando un número de 80-bit en base32, lo cual se traduce en una cadena alfanumérica del tipo "adfr567kfeglñ789" seguidos de una extensión únicamente utilizada en este sistema ".onion"; ya ahondaremos más adelante sobre los mitos y realidades que rodean el resto de supuestos dominios de la DW.

1.3 MEDIDAS QUE FACILITA EL ANONIMATO A LOS USUARIOS

Siguiendo en la misma línea de los dominios web, y haciendo uso de la simple deducción, podemos advertir que la extensión ".com" hace referencia a páginas comerciales, la extensión ".org" a organizaciones, la ".es" a sitios webs pertenecientes a España, la "gov.es" a entidades gubernamentales de España; pero ¿A qué se debe la extensión ".onion"?

Para resolverlo necesitaremos ahondar en el método que facilita el anonimato a los usuarios.

En algún momento de este libro nos hemos comenzado a familiarizar con en el término Tor sin apenas darnos cuenta y ahora sabemos que representa un conjunto de herramientas facilitadoras para la navegación en DW. No olvidemos que Tor es el acrónimo de The Onion Router, o lo que es lo mismo, El Router Cebolla, y aquí es donde nos topamos con ese extraño término de "onion" (del español "cebolla"), porque como una imagen vale más que mil palabras, la alegoría de la cebolla ejemplifica claramente como funciona nuestra herramienta fundamental para el buceo hacia los abismos.

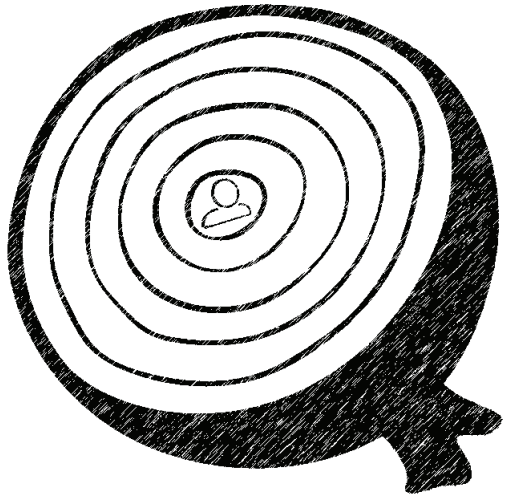


Figura 1. Conexión tipo cebolla. Elaboración propia.

En la capa interna nos encontramos nosotros, los usuarios, y a diferencia de lo que sucede en la SW donde accedemos a una web pasando directamente por la

última sección, en la DW hemos de seguir una línea recta atravesando todas las capas intermedias hasta llegar al exterior.

Cada capa de esta cebolla se denomina nodo, y no son otra cosa más que equipos informáticos capaces de encaminar nuestras peticiones web.

Con una red tipo "cebolla" el anonimato está garantizado, pues la información sale cifrada desde el primer nodo (usuario) y se descifra en el último, mientras que de por medio hay una cadena de encaminadores distribuidas por diferentes países y cada vez que nos conectamos se nos asigna una nueva cadena de nodos con distinta geolocalización. Interesante ¿No?

Es por el funcionamiento intrínseco de la arquitectura de "cebolla", donde todos los nodos reciben y retransmiten la información hasta llegar al final, que notaremos una mayor lentitud en la navegación comparado con un uso convencional en la SW.

1.4 MEDIOS ALTERNATIVOS DE EXPLORACIÓN

Si luego de sumergirnos en la DW en busca del Kraken 2.0 sentimos curiosidad por explorar otros territorios profundos e inhóspitos, existen un par de variaciones que seguramente saciarán nuestro apetito por el redescubrimiento de paisajes poco habituales.

Se tratan de los ecosistemas FreeNet (en adelante FN) e I2P en los cuales ahondaremos lo necesario para que el lector se familiarice con la posibilidad de recorrerlos una vez concluida la presente aventura.

1.4.1 Freenet, la red de túneles olvidados

FN es una solución de software libre ideada para apoyar la libertad de expresión a través de redes de pares y bajo el cobijo brindado por el anonimato.

En esencia su funcionamiento está basado en una red de nodos que comparten un conjunto de información y que siguen una arquitectura del tipo P2P, concepto que conoceremos al detalle en el apartado 2.1 del presente libro.

Para hacernos una idea efusiva de la dinámica dentro de FN vamos a suponer que dentro de una cadena de nodos (equipos) yo represento un llamado *X* y quiero compartir una información *Y* en la red, una vez que comparto esta información ya perdurará dentro de la red independientemente de que *X* siga activo o, dicho de otra forma, *Y* ha sido distribuido por los nodos restantes.

¿Qué tipo de contenido podemos encontrar en FN?

Al igual que en DW encontraremos elementos de diversas temáticas, desde páginas que nos ayuden a navegar, foros de preguntas o contenido aberrante e ilícito, pero tratar esto último en profundidad daría para la confección otro libro instructivo de aventuras en Internet.

1.4.2 I2P, el camino hacia lo invisible

I2P "Invisible Internet Project" es otro sistema en red diseñado para garantizar el anonimato del usuario.

Sí en Tor hablábamos de un funcionamiento multicapas tipo "cebolla", aquí hablamos de un diseño tipo "ajo" en donde no solo se envía un paquete a través de todas las capas (nodos) como ocurre en Tor, sino que cada uno de los mensajes enviados a través del circuido representa una parte (un diente de ajo) del mensaje original.

Otras diferencias sustanciales con respecto a Tor las podemos encontrar en las siguientes características.

- En Tor resulta necesario construir un circuito contra el equipo al que quiere conectase, mientras que en el caso de I2P el mismo túnel de salida sirve para enviar a todos los nodos.
- En Tor no todos los nodos retransmiten tráfico, algunos simplemente son de acceso, mientras que I2P descentraliza su base de datos para repartir la misma carga entre todos los nodos participantes.
- I2P tiene menos ancho de banda que Tor y está menos expandido entre los usuarios que buscan anonimato.

1.5 ÚLTIMA ADVERTENCIA

Con el fin de preservar la identidad de los autores e impedir que el contenido de origen restringido sea accesible y difundido de forma masiva, los archivos multimedia enumerados en el presente libro han sido cuidadosamente editados al objeto de suprimir toda referencia a nombres, direcciones físicas o direcciones web, así como también se ha procedido a censurar rostros y archivos de extrema violencia.

Dada la crudeza de cierto contenido acumulado en el proceso de investigación, el autor se ha reservado el derecho a publicar únicamente los ficheros que pueden

hallarse de una forma extendida y que incluso, en la mayoría de los casos, ya figuran en la SW por otros investigadores.

El autor no se hace responsable del mal uso de la herramienta Tor o de la información publicada en esta obra; hagamos un uso moral y responsable de Internet, y sirva el presente trabajo para difundir un mensaje de advertencia sobre los delitos telemáticos aquí descritos.

Por último, agradecer la labor inconmensurable del GDT (Grupo de Delitos Telemáticos. Guardia Civil) y la BIT (Brigada de Investigación Tecnológica. Policía Nacional) por no bajar nunca la guardia en la lucha contra el material delictivo en las tecnologías de la información y de las comunicaciones.

Ahora que ya sabemos de la existencia del navegador Tor y conocemos el funcionamiento de la DW, cerraremos nuestro KIT de supervivencia para iniciar un viaje a pleno pulmón hacia las profundidades de Internet donde mora el Kraken 2.0.