Término CRIMIPEDIA: Web profunda, darknet y Tor

2016

CRíMINA Centro para el estudio y prevención de la delincuencia

UNIVERSITAS Miguel Hernández

WEB PROFUNDA, DARKNET Y TOR

Olvera Rodríguez, Patricia

RESUMEN

Los avances en tecnología y telecomunicaciones han supuesto muchísimas ventajas para la sociedad, aunque como todo también han traído consigo algunas desventajas o consecuencias. Porque al igual que la sociedad evoluciona y cambia, las formas del crimen y de delinquir también lo hacen.

De esta manera, Internet se ha convertido en un foco de delincuencia con diferentes tipos de cibercriminalidad. Sin embargo, este tipo de criminalidad ha visto cómo crecían sus opciones de expansión y de impunidad gracias a medios que proporcionan anonimato y privacidad en la red, con el uso de navegadores como Tor Browser.

Estos medios mencionados son: la Web profunda (Deep web), la parte más oscura de la red conocida como Darknet (dedicada en gran parte a actividades ilícitos), así como la red Tor.

WEB PROFUNDA

Cuando se desea realizar una búsqueda de información en la red, lo habitual es dirigirse a los motores de búsqueda más conocidos o habituales, tales como Google, Yahoo! Search o Bing, entre otros, arrojando normalmente una gran cantidad de resultados.

Así, se podría pensar que en efecto, cada vez que se realiza una búsqueda, estos motores ofrecen una gran cantidad de resultados (ya si dichos resultados son más o menos acertados sería otra cuestión), o al menos eso es lo que generalmente el usuario podría pensar, pero ¿y si estos resultados fueran tan sólo una pequeña parte de toda la información disponible relacionada con esa búsqueda en la red?

De hecho, llegados a este punto conviene distinguir dos partes diferenciadas en la red o web: por un lado la Web superficial (Surface web), y por otro lado la Web profunda (Deep web).

La primera, la Web superficial, se trata de todo aquel contenido que puede ser indexado por los habituales motores de búsqueda anteriormente mencionados.

La segunda, la Web profunda, en cambio es todo aquel contenido que no puede ser indexado por los habituales motores de búsqueda, es decir serían aquellos contenidos que permanecen fuera del alcance de dichos motores.

Aunque aún no se ha confirmado, se estima que los resultados obtenidos en una búsqueda en la Web superficial representan tan sólo un 4-5% del contenido del total disponible relacionado en la red (Barrera, 2015). Mientras que el 95-96% restante se encuentra ubicado en la Web profunda.

La red presenta varios niveles que varían según los autores, en este caso se optará por uno sencillo de cinco niveles más uno, de López-Barberá (2014):

- **Nivel 0**: Este nivel representa a la web superficial. Donde se encuentra lo que se puede llamar web común (buscadores tipo Google, Yahoo…), es decir contenidos indexados.
- **Nivel 1**: Aquí comienza la web profunda, en este nivel se encontraría contenido como bases de datos, información probada, direcciones,…Es decir, información que no se encuentra indexada pero que no tiene por qué ser nada de contenido ilegal o ilícito.
- **Nivel 2**: En este nivel ya comienzan las páginas de carácter ilegal como pornografía o resultados de búsqueda bloqueada por otros servidores.
- **Nivel 3**: Para este nivel se hace necesario el uso de proxy. En este nivel se encuentra temas peligrosos que ya se encuadran dentro del cibercrimen. Desde pornografía infantil, grupos de intercambio de materiales, virus…
- **Nivel 4**: A este nivel también se le conoce como "Charter Web" o darknet. Los denominados ".onion". En este nivel hay necesidad de utilizar el navegador Tor. Aquí se encuentra pornografía de cualquier tipo, asesinatos reales, secuestros y torturas, tráfico de órganos, intercambio de divisas, hackers, documentos de anonymous, tráfico de armas, intercambio de drogas, etc. Conforma el mercado negro más grande que se ha visto hasta la fecha.
- **Nivel 5**: También conocido como "Marianas Web", cuyo nombre deriva de la fosa oceánica de las Marianas, la más profunda conocida. Se dice que es lo más profundo a lo que se puede llegar dentro de la red, el denominado nivel prohibido, donde no se puede confirmar el contenido, pero donde muchos dicen que agencias de inteligencia y gobiernos guardan informaciones secretas.

Si bien es cierto que apenas se tiene conocimiento del nivel 5, otros autores, como Albarracín (2016), añaden tras este nivel 5 otros tres más:

- **Nivel 6**: Conocido como "The Fog" (la niebla en castellano). En este nivel los hackers que consiguen entrar utilizan la computación cuántica para poder sobrepasar la encriptación. No existen pruebas concretas de que alguien haya conseguido acceder a él, y el contenido del mismo es cuanto menos confuso.
- **Nivel 7**: También conocido con el sobrenombre de "Virus Soup". A este nivel sólo acceden hackers experimentados que evitan el acceso de los que van en niveles anteriores al mismo.

- **Nivel 8**: El nivel "The Primarch System". Si el contenido de los dos niveles anteriores eran confusos, en éste ya se tratan de puras especulaciones donde se cree que contiene el control primario del mismo Internet. Para su acceso se requieren equipos y conocimientos especiales de encriptación.

DARKNET

La primera vez que se hizo referencia al término Darknet, fue de la mano de cuatro investigadores de Microsoft en 2002, que lo definieron como:

Un conjunto de redes y tecnologías utilizadas para compartir contenidos digitales. Darknet no es una red física independiente, sino una aplicación y capa que funciona en las redes ya existentes (Biddle, England, Peinado & Willman, 2002).

Si bien cabe añadir que desde entonces, esta concepto ha evolucionado mucho. Así, de forma errónea, muchos autores y usuarios tienden a confundir los términos Web profunda (Deep web) y Darknet, pensando que son términos sinónimos e intercambiables entre sí. Pero lo cierto es que son términos diferentes y el hecho de que se traten como uno sólo puede crear confusión, especialmente entre usuarios o lectores principiantes en el tema.

Así pues, antes de continuar, conviene diferenciar ambos conceptos: la Web profunda, como se ha comentado anteriormente, se trata del contenido que se encuentra oculto a la vista y que en realidad no puede ser buscado e indexado con la misma facilidad y fiabilidad que el indexado. Por otro lado, Darknet es tan sólo una parte de la Web profunda, en concreto, se trata de aquella parte de la web profunda que recibe su nombre precisamente por el tipo de contenido que se encuentra en ella: pornografía infantil, venta de drogas, venta de armas, sicarios, etc.

Tal y como se ha definido el término Darknet, queda claro que no se trata de ninguna red, sino de un conjunto de contenidos de carácter ilegal e ilícito ubicados dentro de la Web profunda.

¿Cómo se accede entonces a Darknet y por ende a sus contenidos?

Existen diferentes medios y formas de acceder a ella, a continuación se comentarán las principales y más utilizadas, conocidas también como Cipherspace.

- **Freenet.** Se trata de un software libre y una red de distribución de información descentralizada y resistente a la censura. Tiene como objetivo proporcionar libertad de expresión a través de las redes P2P mediante una fuerte protección del anonimato. Su diseño se basa en una red P2P no estructurada de nodos no jerarquizados que transmiten entre ellos mensajes y documentos, y su funcionamiento se basa en almacenar documentos y permitir su acceso posterior por medio de una clave asociada, impidiendo que sea posible la censura de los documentos y ofreciendo anonimato tanto al usuario que lo publica como al que lo descarga.

- **I2P.** Siglas del término en ingles Invisible Internet Project (Proyecto de Internet Invisible) Se trata de un software y una red, la cual ofrece una capa de abstracción para las comunicaciones entre ordenadores, permitiendo así la creación de herramientas y aplicaciones de red con un fuerte anonimato. Este tipo de red está basada en el concepto de túneles entrantes y salientes, lo cual ofrece facilidad para la adaptación de programas persistentes a la red I2P. Cabe decir que se adapta muy bien a las redes P2P. Es un software libre y utiliza varias licencias libres.

- **ZeroNet.** Se trata de un software y una red descentralizada, como las redes P2P, además es de código abierto, por lo que se trata de un software desarrollado y distribuido libremente. Por defecto no se trata de un servicio que proporcione anonimato, si no que se debe utilizar algún complemento como Tor. Si bien las direcciones de los sitios web son específicas y especiales de la plataforma, se pueden visitar y acceder a ellas sin problema con un navegador convencional siempre y cuando se utilice la aplicación Zeronet, que actúa como un servicio de hosting local para este tipo de páginas.

- **Tor.** Se trata de un software y una red basados en el enrutamiento de cebolla, y cuyo objetivo principal es el anonimato del usuario durante su navegación y uso de la red de redes Internet.

TOR

Tor (The Onion Router), debe su nombre a la forma en la que funciona. Su traducción literal sería encaminamiento de cebolla, y se trata de una implementación de dicho tipo de enrutamiento/ encaminamiento.

Se trata de una red que ayuda al usuario a poder utilizar Internet de forma anónima. En concreto, Tor oculta el origen y el destino del tráfico en Internet del usuario, lo cual impide que alguien ajeno pueda saber tanto quién es como lo que está buscando éste (a pesar de que se conozca alguno de los dos). El hecho de que Tor oculte también el destino de su tráfico permite que se puedan eludir de esta manera algunas formas de censura.

Desde la página oficial Tor Project se facilita la siguiente definición:

Es un software libre y una red abierta que ayuda al usuario a defenderse del análisis del tráfico, vigilancia que amenace la libertad personal y privacidad, confidencialidad en los negocios y relaciones, y la seguridad del Estado (Tor Project, n.d.).

El proyecto de la red Tor pertenece a la tercera generación de enrutamiento de cebolla, y ha pasado por diferentes etapas desde su inicio. La primera versión de éste fue anunciada en Septiembre de 2002 por sus creadores (Dingledine, Mathewson y Syverson).

Fue financiado y desarrollado como un proyecto de enrutamiento de cebolla de tercera generación del Naval Research Laboratory (Laboratorio de Investigación Naval). Desarrollado originalmente junto con la U.S. Navy (Armada de Estados Unidos), con el propósito principal de proteger las comunicaciones gubernamentales. Pero una vez que se terminó dicha financiación, en 2004 tomó su relevo la Electronic Frontier Foundation que la financió a lo largo de todo ese año hasta finales del año 2005. Desde entonces el proyecto Tor sobrevive gracias a las donaciones de diferentes organizaciones. En la actualidad, el proyecto se encuentra bajo la tutela de la organización sin ánimo de lucro Tor Project.

Tor ha sido desarrollado durante muchos años, consiguiendo así un producto con mucha estabilidad. Además, es considerada como una de las mejores herramientas de privacidad existentes en la actualidad.

A pesar del propósito original de la Armada de los Estados Unidos para la red Tor que no era otro que el de proteger las comunicaciones gubernamentales, hoy en día, es utilizada a diario para una amplia variedad de propósitos por militares, periodistas, policías y activistas, entre otros.

Tal y como se ha comentado anteriormente, el objetivo de Tor es ofrecer anonimato y privacidad en la navegación al usuario. Para ello, Tor intercepta el tráfico de red desde una o más aplicaciones en el equipo, generalmente desde el navegador web, y lo mezcla a través de un número de equipos escogidos al azar antes de enviarlo a su destino.

Esto hace que se oculte su ubicación, por lo que se hace más difícil para los servidores identificarle en repetidas visitas, o incluso enlazar visitas independientes a diferentes sitios web, lo que hace que el seguimiento y la vigilancia se vuelvan más difíciles.

Los equipos utilizados para el uso en la red Tor se conocen como nodos (relays), y son proporcionados por voluntarios de todo el mundo. Se cree que ya son unos 7000 a comienzos del presente año 2016 (Ducklin, 2016).

¿Cómo funciona realmente?

Antes de que un paquete de datos se envíe a través de la red, el ordenador elige una lista aleatoria de nodos y encripta de forma repetida los datos en múltiples capas, como una cebolla.

Cada nodo conoce sólo lo suficiente para quitar la capa de encriptación más externa, para pasar después lo que queda al siguiente nodo de la lista o circuito.

A modo de ejemplo, se podría pensar en ello como si enviáramos una postal dentro de varios sobres, uno dentro de otro, con una dirección diferente en cada sobre, para luego enviarlo todo como un único sobre. Algo así como una muñeca rusa, que cada una de ellas contiene a las anteriores, y así sucesivamente.

Siguiendo con el ejemplo, la persona que recibe el sobre en primer lugar, el más externo, sólo sabrá quién le ha enviado el sobre y a quién debe enviárselo, ya que aparece la dirección en el sobre que estaba dentro del que él recibió, a su vez, el siguiente receptor del mensaje sólo sabrá quién se lo ha enviado y a quién le debe enviar el contenido de su sobre, pero no sabrá el contenido de la postal ni el resto de integrantes de la cadena hasta que llegue al receptor final, así ocurrirá sucesivamente hasta que llegue la postal al receptor final, el cual sabrá quién le envió el mensaje y el contenido de la postal, pero no la ruta que siguió la postal ni tampoco quién la comenzó.

Pero además, Tor permite ver el contenido oculto en Internet, conocido como la red profunda. Esto se debe a que al igual que un usuario podría navegar de forma anónima el resto de usuarios podrían mostrar información de la misma manera. Si es tan difícil de rastrear, entonces, ¿cómo se puede acceder a dichos sitios anónimos? La respuesta es sencilla, a través de una "onion address". Ésta se compone de una serie de letras y números al azar, como por ejemplo la versión limpia (sin censura) de Wikipedia, a la cual se accedería mediante la siguiente URL: 3suaolltfj2xjksb.onion

Esta URL no funcionará a menos que se esté utilizando un navegador compatible con la red Tor. E incluso en el remoto caso de que se consiguiera acceder al sitio sin dicho navegador, la mayoría de la información se mostraría inaccesible.

Esta "onion address" se utiliza para encontrar el servidor dentro de la red Tor. Como las direcciones no apuntan a una dirección real en Internet, no hay forma de acceder totalmente al contenido sin Tor. Existen otras herramientas que permiten acceder a direcciones anónimas, pero de esta manera el usuario pierde uno de los principales beneficios de Tor, que no es otro que el de ocultar su identidad, además de que el contenido a menudo puede ser censurado.

A parte del navegador Tor Browser, existen otras aplicaciones y software que permiten el acceso a la red Tor, como por ejemplo Tor2Web, Whonix o Tails.

TIPOS DE USUARIOS DE ESTOS MEDIOS

Tal y como se ha comentado anteriormente, si bien en sus inicios la red Tor tenía como objetivo proteger las comunicaciones gubernamentales y por tanto, sus usuarios serían la propia U.S. Navy y el gobierno de Estados Unidos en todo caso, en la actualidad se utiliza para una amplia variedad de propósitos y por personas de diversos perfiles.

- **Militares**: Monitorizar el tráfico de Internet para descubrir lugares de interés militar (agentes de campo), servicios ocultos, recogida de información (evitar la localización revelando la vigilancia) en lugares controlados por insurgentes.
- **Profesionales de TI**: Verificar reglas de cortafuegos, pasar por alto sus propios sistemas de seguridad por un motivo justificado, pruebas de funcionamiento de la red, acceder a recursos de Internet (saltándose las restricciones de acceso de la propia empresa).
- **Ejecutivos y jefes de negocio**: Evitar brechas de seguridad de información de cámaras de compensación, observar a su competencia libremente, mantener estrategias confidenciales, responsabilidad (libertad para denunciar malversación interna).
- **Activistas y denunciantes**: Activistas de derechos humanos utilizan Tor para denunciar de forma anónima abusos en las zonas de peligro. Proporciona la capacidad de evitar la persecución pudiendo denunciar hechos injustos. Denunciar y revelar información de talleres clandestinos en el este de Asia que producen bienes para países occidentales. Puede evitar la censura corporativa.
- **Criminales**: Aprovechan el anonimato de la red para delinquir de diversas formas: pedofilia, pornografía infantil, ciberacoso, venta de drogas, etc.
- **Policía**: Vigilancia en línea, operaciones sorpresa, seguir líneas de pistas de forma anónima.

- **Periodistas**: Periodistas residentes en China la utilizan para escribir sobre eventos locales que fomenten el cambio social y la reforma política, investigaciones de propaganda

estatal y publicar historias no controladas por el Estado evitando el riesgo de sufrir consecuencias personales.

- **Ciudadanos en países con censura**: Los ciudadanos que vivan en países opresores y/o con censura tienen libertad para poder consultar información y expresar su opinión, e incluso denunciar alguna situación política saltándose la censura.
- **Blogueros**: A menudo los blogueros son despedidos de sus trabajos por expresar libremente su opinión e información totalmente legal, la cual puede no ser políticamente correcta. Por ello utilizan Tor para disfrutar del anonimato que ofrece.
- **Gente normal**: Protegen su intimidad de vendedores sin escrúpulos y ladrones de identidad (evitando que los ISP vendan sus registros de navegación en Internet), protegen sus comunicaciones de las empresas irresponsables, protegen a sus hijos en líneas, investigación de temas sensibles en determinados países (SIDA, control de natalidad, etc.), evita vigilancia, sirve para eludir censura (por ejemplo si tiene bloqueado Facebook o YouTube en su país).

Generalmente circula la idea, en parte equivocada, de que la red Tor es sinónimo de ciberdelincuencia y actividades ilícitas, cuando la red Tor es utilizada para diferentes fines y por distintos tipos de personas. Aunque también es cierto que por las características de anonimato y privacidad que brinda al usuario la red facilita en cierta forma que se puedan cometer actos ilícitos sin temor a las repercusiones o con impunidad.

TIPOS DE DELITOS Y/O ABUSOS QUE SE COMETEN POR ESTOS MEDIOS

Aunque estos tipos de medios hayan perseguido desde sus inicios como propósito principal el anonimato y privacidad de los usuarios, muchos criminales aprovechan

las ventajas que les proporcionan dichos medios para delinquir, debido a la dificultad que supone rastrearlos y localizarlos en este tipo de medios.

A continuación se nombran algunos de los delitos más comunes que se dan en dichos medios:

Tráfico de drogas.

A través de diferentes lugares de venta llamados market place, en los que se puede encontrar prácticamente de todo, aunque uno de los productos estrella es la droga. Los vendedores y compradores de drogas han encontrado en este tipo de medio el lugar perfecto para distribuir y comprar este tipo de sustancias. Al más puro estilo de plataformas como Ebay, diferentes market place ofrecen una gran variedad de sustancias y estupefacientes ilícitos, divididas por categorías: esteroides, disociativos, estimulantes, etc. Drogas como cocaína, burundanga o hachís figuran entre los muchos productos disponibles. Aunque también medicación como oxidocona o xanax se ofertan en este tipo de portales. Y no sólo sustancias, también se venden materias primas y utensilios para el abastecimiento de los productores de drogas.

Uno de los mercados más populares fue Silk Road, que aunque se desmanteló su versión 2.0 en 2013 con la detención de su creador, otros mercados han seguido su estela y se han hecho con sus clientes y vendedores. Cabe decir que Silk Road resurgió a principios del presente año con su versión 3.0.

Si bien es cierto que este tipo de sitios web cambian y desaparecen a menudo, existen páginas que recogen y actualizan los diferentes market place disponibles, actualizandolas con bastante frecuencia. Además, muchos de estos sitios web han establecido un sistema por invitación, de manera que necesitas una para poder acceder a los servicios que ofrecen y realizar transacciones en dicho sitio, de esta manera pueden llevar cierto control y publicitarse solo en aquellos sitios que consideren seguros para sí mismos.

Pedofilia y pornografía infantil.

Antes de Internet, el intercambio o la recopilación de imágenes de niños desnudos seguramente era una tarea bastante difícil y peligrosa para pederastas y pedófilos, pero con el auge de Internet, la evolución y servicios que ofrecen ciertos medios de acceso a la red

como la darknet, Internet se ha convertido en un lugar de fácil y rápido acceso a contenidos de este tipo.

En concreto, la darknet debido al carácter anónimo que presenta, se convierte en el foro ideal para la pederastia, en el que criminales de todo el mundo pueden compartir su material bajo diferentes sobrenombres, como por ejemplo “hard candy”.

Venta ilegal de armas.

Al igual que el tráfico de drogas, el negocio de venta ilegal de armas, ha encontrado una gran plataforma de venta en la darknet. De nuevo, el anonimato del medio proporciona un plus para la venta, en este caso la venta ilegal de armas.

Muchos de los market place mencionados para la venta y tráfico de drogas, también ofrecen productos para los compradores y vendedores de este mercado ilegal.

La amplia variedad de armas que se ofrecen en estos mercados es cuanto menos sorprendente. Desde pistolas, fusiles o granadas hasta diseños para impresoras 3D de pistolas.

Sicarios.

Los asesinos a sueldo encuentran en la darknet un medio perfecto donde publicitarse y ofrecer sus servicios.

Los precios de este tipo de servicios varían en función de diferentes variables. Las cuales pueden ser desde el país de residencia (tanto del sicario como del objetivo), costes de desplazamiento, la importancia del objetivo o futura víctima (figuras públicas, políticos o empresarios importantes), el tiempo para la realización del trabajo, la edad del objetivo, etc.

Algunos ofrecen servicios extras, como por ejemplo el envío de una foto del cadáver al contratante del servicio. Servicios extras que por supuesto hay que sumar al precio del servicio.

Otros incluso tienen algunas excepciones como no matar a menores de 16 años o políticos de altos cargos.

Si bien es cierto que también se encuentra mucho farsante entre los anunciantes de este servicio, tampoco es difícil encontrar uno si se necesita. Algunos trabajan por separado y otros en grupo.

Venta de pasaportes falsos y falsificaciones.

Conseguir un pasaporte falso en la darknet no es difícil, pero tampoco es barato. Los precios varían, dependiendo del país del que se quiera el pasaporte. Muchas veces depende también de cómo de buena tenga que ser la falsificación, en función de los detectores que tenga cada país para su detección, para que parezca original.

Además de los pasaportes también se ofrecen falsificaciones como pueden ser carnés de conducir o incluso dinero.

Localización, acoso y extorsión.

En estos medios hackers ofrecen sus servicios para localizar a personas, ya sea a través de su teléfono móvil o a través de otros medios.

Esta localización puede ser utilizada para diferentes fines que se podrían catalogar si bien no como benignos tampoco como los peores, como puede ser localizar a algún vendedor que protagonizó algún timo o algún pariente. Pero también puede ser realmente peligroso, como por ejemplo puede ser la de una víctima de maltrato buscada por su expareja.

El cyberstalking, se trata del uso de Internet u otra tecnología de comunicación para hostigar, perseguir o amenazar a alguien (Basu y Jones, 2007). Por lo que ni que decir tiene, que gracias de nuevo al anonimato, se encuentra en estos medios la forma perfecta para que los cyberstalkers realicen sus actividades de persecución y amenaza contra sus víctimas, sin temor a las represalias.

Respecto a los menores, a parte de los ya mencionados, se dan además otros tipos de delitos relacionados con el ciberacoso. Como es el caso del cyberbullying, el cual también aprovecha las ventajas de anonimato que le ofrecen estos medios. Pues se trata de un tipo de acoso online, y una de las formas más comunes de agresión entre menores. Otro fenómeno relacionado con menores que se da en este tipo de medios es el online grooming, en el que los pederastas y pedófilos contactan con víctimas (menores de edad) y mantienen comunicación con ellas a través de chats, fingiendo ser una persona cercana y con inquietudes afines, ganándose así su confianza. Una vez conseguida, le solicitan que le envíen fotografías

o vídeos de ellos desnudos, para más tarde y una vez conseguido el material explícito, chantajearlos con la difusión de dicho material para que accedan a sus peticiones. Hay que añadir que este tipo de comportamientos se dan sin necesidad de utilizar medios como darknet, principalmente porque las víctimas no suelen tener este tipo de conocimientos informáticos como para acceder a la darknet por medio de navegadores especiales.

Terrorismo.

Grupos terroristas, especialmente yihadistas, utilizan estos medios para congregar y comunicarse con sus militantes.

Sitios dedicados a la divulgación de la ideología yihadista, o incitando a alistarse al ejército para lo que ellos mismos denominan como la guerra santa, se alojan en la darknet. Incluso recaudan fondos mediante el uso de bitcoins. Existen sitios web que piden donaciones para su causa, y además enseña a los militantes y simpatizantes a comprar armas para la yihad en Darknet.

Estas organizaciones terroristas, como por ejemplo Al qaeda o el ISIS, suelen tener una web a modo de señuelo, alojada normalmente en la web superficial, y que contienen material sin importancia de divulgación y llamamiento a la ideología que defienden. Esta táctica es utilizada para que las fuerzas de seguridad crean que esas son sus páginas de difusión reales, mientras que las organizaciones operan en otras situadas en Darknet, evitando o al menos intentando evitar que las autoridades lleguen hasta sus sitios web de importancia.

Hacktivismo.

Si los criminales encuentran perfectos este tipo de medios para delinquir, sin duda, los que están en lo que se podría decir en su hábitat natural son los denominados hackers.

Este tipo de delincuentes se reúnen en diferentes organizaciones para operar en grupo. Muchos de ellos bien conocidos, como por ejemplo Anonymous. Se supone que su filosofía es siempre la de hacer el bien o lo correcto según su moral, el problema reside en que no siempre lo que se califique como correcto sea legal.

Casos como el de WikiLeaks, que destapó documentación del estado norteamericano, o como la violación masiva de datos de Sony, publicando los datos de las cuentas de muchos usuarios

de Playstation, han sido de los que más repercusión han causado en los medios de comunicación y en la opinión pública.

La comunicación entre los integrantes de estos grupos u otros hackers se suele dar en foros en los que sólo se puede acceder por invitación.

Malware.

Se trata de programas maliciosos, instalados normalmente sin el consentimiento o al menos sin que el usuario sea consciente realmente de lo que está instalando en su equipo.

El uso de las botnets unido al malware, en este tipo de medios en los que se goza de cierto nivel de privacidad y sobre todo, anonimato, ha crecido mucho con respecto a los situados en la web superficial.

Aprovechando las posibilidades de anonimato que ofrece la red Tor, cualquier tráfico generado por el malware que intente ser analizado y capturado por autoridades o investigadores, resultará complicado de rastrear para capturar a los ciberdelincuentes.

Y ya no sólo los PCs o móviles son susceptibles de este tipo de ataques, si no que prácticamente cualquier dispositivo con conexión a Internet, es susceptible de ser contaminado o contagiado por algún tipo de malware.

Un tipo de malware bastante utilizado en los últimos años es el conocido como ransomware, este software malicioso infecta un determinado PC elegido por el ciberdelincuente y le da la capacidad a éste de bloquearlo desde una ubicación remota e incluso encriptar los archivos quitándole el control de toda la información y datos almacenados al usuario, al que normalmente el delincuente devolverá el control e información requisada siempre a cambio de una cantidad monetaria estimada por el ciberdelincuente.

Piratería.

La descarga de contenidos siempre ha sido uno de los estandartes de la darknet, de hecho anteriormente la definición de dicho término se relacionaba estrechamente con el intercambio y distribución de materiales y contenidos protegidos por derechos de autor y distribución

(copyright). En la actualidad las leyes de la mayoría de los países se han endurecido para perseguir las descargas ilegales y la piratería en la red, por lo que los contenidos que eran tan fáciles de encontrar en la Web superficial antes, ahora es necesario buscarlos en sitios más recónditos alojados en la web profunda e incluso en la darknet. Pudiéndose encontrar un mundo lleno de contenidos disponibles para su posterior descarga ilegal. Desde libros, películas o música a software o programas de pago. A través de aplicaciones de descarga o de servidores destinados a ello.

Revelación de documentación secreta y/o confidencial.

El robo y posterior revelación de información confidencial y secreta a diferentes gobiernos y empresas por parte de varios grupos de hackers ha sido uno de los motivos de la creciente popularidad de estos medios, especialmente de la darknet.

Casos, como por ejemplo el de Wikileaks (nombrado anteriormente) o el caso Snowden, en el que un antiguo consultor e informante de la CIA y NSA, desveló información secreta a través de diferentes periódicos de documentos clasificados como alto secreto sobre varios programas de las organizaciones con las que trabajó y colaboró.

Otros caso es el también antes enunciado robo de datos de la empresa Sony, en el que muchos usuarios vieron cómo los datos de sus cuentas de PlayStation eran publicadas en Internet.

A parte de los delitos nombrados, existen otros como por ejemplo las películas denominadas “snuff”, en las cuales se filman violaciones, torturas, suicidios o asesinatos, entre otros. También, aunque en menor medida, circula otro tipo de material que podría calificarse como poco de excéntrico, como vídeos de carácter escatológico o incluso “crush fetish”, en las cuales se puede ver el maltrato y asesinato de animales aplastándolos.

TIPOS DE DELITOS Y/O ABUSOS QUE SE PREVIENEN POR ESTOS MEDIOS

Si bien este tipo de medios permiten y facilitan que se cometan ciertos delitos, también ayudan a prevenir otros. Como por ejemplo:

- **La protección de testigos y/o víctimas de abuso doméstico o ciberbullying.** Protegiéndose de esta manera, e incluso previniéndose de posibles acosadores.
- **Denunciar delitos.** Proporcionar información sobre la comisión de delitos de forma anónima.
- **Denunciar delitos dentro de la propia darknet.** Existen organizaciones de madres en Estados Unidos que se dedican a localizar todo tipo de redes de pedofilia y pornografía infantil para su posterior denuncia.
- **Derecho a la información.** Para evadir la censura en países como Siria o China, entre otros, pudiendo acceder a la información del resto del mundo de forma más segura.

TEMAS RELACIONADOS

Cibercrimen

Este fenómeno engloba los delitos que se pueden cometer exclusivamente en el entorno del ciberespacio, y por ende de la informática y de Internet, así como otros delitos que pueden ser cometidos sin la necesidad de esos medios, pero que se incluyen aquí cuando son cometidos mediante los mismos.

Crimen organizado

Grupos organizados de forma social con el fin de desarrollar actividades delictivas y que éstas reporten un beneficio, generalmente económico. Actividades como tráfico de drogas, trata de blancas o venta ilegal de armas, entre otros, son algunas de las más habituales.

Extorsión

Presión que se ejerce sobre alguien mediante amenazas para obligarlo a actuar de determinada manera y obtener así dinero u otro beneficio.

Pedofilia

Atracción erótica o sexual que una persona adulta siente hacia niños o adolescentes.

Terrorismo

Actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos.

Tráfico de drogas

Delito que consiste en cultivar o elaborar drogas tóxicas y comer ciar con ellas sin los controles legales.

BIBLIOGRAFÍA

Agencia EFE (2015, 30 de Mayo). Cadena perpetua para el creador de Silk Road, la web que vendió 200 millones de dólares en drogas ilegales. *ABC* . Extraído el 8 de Julio de 2016 desde http://www.abc.es/internacional/20150530/abci-cadena-perpetua-vender-drogas-201505300020.html

Albarracín, S. (2016). La Deep Web: ¿Qué es y cuáles son sus niveles?. *El Vínculo Digital*. Extraído el 4 de Agosto de 2016 desde http://www.elvinculodigital.com/que-es-la-deep-web/

Basu, S. & Jones, R.P., (2007). *Regulating Cyberstalking*. JILT, 2007 (2). Extraído el 13 de Agosto de 2016 desde http://go.warwick.ac.uk/jilt/2007_2/basu_jones/

Bergman, M.K., (2001, Agosto). White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing, 7 (1).* Extraído el 2 de Junio de 2016 desde http://dx.doi.org/10.3998/3336451.0007.104

Biddle, P., England, P., Peinado, M., & Willman, B. (2002). The Darknet and the Future of Content Distribution. *Microsoft Corporation*. Extraído el 6 de Agosto de 2016 desde https://crypto.stanford.edu/DRM2002/darknet5.doc

Byrne, B.P. & Schwartz, O. (2016, 5 de Enero). *How Criminals Can Buy Guns On The Dark Net.* http://www.vocativ.com/267755/how-criminals-can-buy-guns-illegally-on-the-dark-net/

Duckin, P. (2016). *What is…Tor*. Extraído el 19 de Febrero de 2016 desde https://blogs.sophos.com/what-is/tor/

El rincón del crimen en la red: la web oscura sin descubrir.(2016, 15 de Febrero). Extraído el 8 de Julio de 2016 desde http://www.bittin.co/el-rincon-del-crimen-en-la-red-la-web-oscura-sin-descubrir/

Farrell, J. (2016, 10 de Marzo). Inside the Dark Net: Digitizing the cure for childe pornography. *Preda Foundation.* Extraído el 13 de Agosto de 2016 desde http://www.preda.org/world/inside-the-dark-net-digitizing-the-cure-for-child-pornography/

Fernández, R. J., & Ruiz, E. (2016). Deep Web: el lado oscuro de Internet. *Red seguridad, 73,* 64-65. Extraído el 23 de Agosto de 2016 desde http://www.redseguridad.com/revistas/red/073/index.html#65/z

González, G. (2015). *Surface web, Deep web y Darknet: ¿en qué se diferencian?*. Extraído el 4 de Agosto de 2016 desde

http://blogthinkbig.com/surface-web-deep-web-darknet-se-diferencian/

Libicki, M. C., Romanosky, S., Tkacheva, O., & Winkelman, Z. (2015). Internet Freedom Software and Illicit Activity. Supporting human rights without enabling criminals. *Rand Corporation*. ISBN: 978-0-8330-9110-9. Extraído el 2 de Julio de 2016 desde http://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1151/RAND_RR1151.pdf

López-Barberá, A. (2014, Abril). Deep Web o Internet profundo. *Seguritecnia, 407*, 96-97. Extraído el 3 de Julio de 2016 desde http://www.seguritecnia.es/revistas/seg/407/index.html#97/z

Miró, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*, 13-07. Extraída el 6 de Agosto de 2016 desde http://criminet.ugr.es/recpc/13/recpc13-07.pdf

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Pagnotta, S. (2014). *Navegación anónima en Tor: ¿herramienta para cuidadosos o para cibercriminales?*. Extraído el 3 de Julio de 2016 desde http://www.welivesecurity.com/la-es/2014/07/02/navegacion-anonima-tor-herramienta-cuidadosos-o-cibercriminales/

Pascual, A. (2013). Deep Web, un paseo por los bajos fondos de Internet. *El confidencial*. Extraído el 10 de Febrero de 2016 desde http://www.elconfidencial.com/tecnologia/2013-04-09/deep-web-un-paseo-por-los-bajos-fondos-de-internet_767430/

Quintin, C. (2014). *Tor is For Everyone: Why You Should Use Tor*. Extraído el 10 de Febrero de 2016 desde http://gizmodo.com/tor-is-for-everyone-why-you-should-use-tor-1591191905

Real Academia Española. Diccionario de la lengua española, 23º Edición (Octubre de 2014). www.rae.es

Schneier, B. (2007, 20 de Septiembre). *Anonymity and the Tor Network*. Extraído el 7 de Agosto de 2016 desde https://www.schneier.com/blog/archives/2007/09/anonymity_and_t_1.html

Schultz, D. (2012). *A Tor of the Dark Web*. Extraído el 2 de Junio de 2016 desde https://slifty.com/2012/08/a-tor-of-the-dark-web/

Sui, D., Caverlee, J., & Rudesill, D. (2015). The Deep Web and the Darknet: A look inside the Internet's massive black box. *Science Technology Innovation Program, 3*. Wilson Center. Extraído el 8 de Agosto de 2016 desde https://www.wilsoncenter.org/publication/the-deep-web-and-the-darknet

Syverson, P. (2011). A Peel of Onion. *Center for High Assurance Computer Systems. U. S. Naval Research Laboratory*. Extraído el 6 de Agosto desde https://www.acsac.org/2011/program/keynotes/syverson.pdf

Tor: Overview. (n.d.). Extraído el 19 de Febrero de 2016 desde https://www.torproject.org

Trend Micro (2011, 31 de Octubre). *Hacktivism: The good, bad and ugly of cybercriminals with a message (op/ed)*. Extraído el 7 de Agosto de 2016 desde http://blog.trendmicro.com/hacktivism-the-good-bad-and-ugly-of-cybercriminals-with-a-message/

NOTAS

Ilustración 1
Océano de la información en la red.

*Fuente: http://www.brandpowder.com/how-deep-is-your-web