Departamento de Seguridad Informática MINSAP

Febrero 2017

Volumen 1, nº 1

Contenido:

Estos son los nuevos ataques informáticos que aparecerán en 2017 1

Deep Web, Dark Web y Darknet: éstas son las diferencias. 2

Deep Web, Dark Web y Darknet: éstas son las diferencias. 3

Ataques al DNS: cómo intentan dirigirte a páginas falsas. 4

Puntos de interés especial:

-Los ataques Phlashing se caracterizan por enviar una gran cantidad de información a los sistemas generando en los servidores una carga tan elevada que terminará dañando físicamente el hardware.

-La porción de Internet que **está intencionalmente oculta a los motores de búsqueda**, usa direcciones IP enmascaradas y es accesible sólo con un navegador web especial

-El sistema de nombres de dominio DNS es lo que nos permite **resolver el nombre de una página web por su dirección IP**.

Estos son los nuevos ataques informáticos que aparecerán en 2017

2016 no se ha caracterizado precisamente por ser un año donde haya destacado la seguridad informática, sino más bien todo lo contrario. A lo largo de todo el año hemos podido ver todo tipo de ataques informáticos, desde malware, concretamente ransomware, cada vez más peligroso, hasta las nuevas redes de dispositivos zombie, como parte del IoT, capaces de llevar a cabo ataques DDoS de hasta 1 Tbps, los ataques más rápidos de la historia. 2017 no tiene pinta de mejorar en este aspecto.

Varios expertos de seguridad están empezando a dar forma a nuevos ataques informáticos a los que podríamos tener que enfrentarnos a medida que avanza el año. Por ejemplo, un nuevo concepto de ataque informático al que tendremos que enfrentarnos será al nuevo **Permanent Denial of Service, o PDoS**.

¿Qué son los ataques PDoS?

También conocidos como ataques **Phlashing,** estos ataques informáticos se caracterizan por enviar una gran cantidad de información a los sistemas de las víctimas para que estos la procesen. Estos ataques generarán en los servidores una carga de trabajo tan elevada durante un largo periodo de tiempo que, al final, **terminarán dañando físicamente el hardware de la víctima**, obligando a cambiar la pieza afectada.

Obviamente, estos ataques no van a estar destinados a servidores o centros de datos ya que la capacidad de proceso de estos es muy elevada, sino que sus objetivos serán, principalmente, routers impresoras, televisores y cualquier otro dispositivo que forme parte del IoT que, al tener una capacidad de proceso más reducida tiene una mayor probabilidad de terminar siendo dañado.

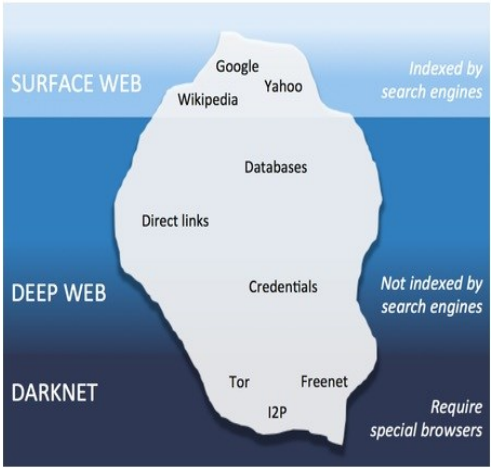
Los ataques PDoS más benevolentes se centrarán solo en **corromper el firmware** de los dispositivos, algo sencillo de reparar si se vuelve a instalar el mismo, aunque los más agresivos llegarán incluso a dañar físicamente el dispositivo.

Otros dos nuevos conceptos que probablemente ganen gran protagonismo a lo largo de este año son los **Advanced Persistent Denial of Service (APDoS)**, los ataques de denegación de servicio persistentes y, sobre todo, los ataques **Telephony Denial of Service (TDoS)**, un tipo de ataque informático capaz de causar grandes estragos en la red causado por una serie de llamadas continuas sin respuesta.

La Darknet ganará también mucha popularidad como red distribuida para llevar a cabo ataques informáticos.

Si un ataque informático se está realizando desde una dirección IP concreta, o desde una red más o menos delimitada (por ejemplo, desde un país concreto), es relativamente sencillo hacer frente a esos ataques y bloquearlos. Sin embargo, si el ataque es distribuido, utilizando, por ejemplo, la red Tor, la cosa se complica, y mucho.

Deep Web, Dark Web y Darknet: éstas son las diferencias.



El término Deep Web fue acuñado por la empresa especialista en indexado 'Bright Planet', y lo utilizaron **para describir contenidos no indexables** como las solicitudes de bases de datos dinámicas, los paywalls y otros elemento difíciles de encontrar mediante el uso de buscadores convencionales. Pero más tarde llegó el caso de Silk Road, y los medios de comunicación empezaron a utilizar ese término para referirse a otros elementos como las Dark Webs.

Bright Planet ha defendido en muchas ocasiones que el término Deep Web es inexacto para referirse a las Dark Webs y Darknets, pero el daño ya estaba hecho, la gente lo había asimilado y **distinguir estas tres nomenclaturas se ha convertido en un infierno**. Por eso, hoy vamos a intentar dejar estos tres conceptos para saber cuales son exactamente las diferencias y a qué nos referimos con ellos. Por lo general, para distinguir los conceptos de Darknet, Deep Web y Surface Web o web superficial suele utilizarse el esquema del iceberg. La punta, **lo poco que sobresale en la superficie es la web tal cual la conoces**, la Surface Web. Todo lo que hay debajo del agua es la Deep Web, y la parte más profunda de ella es la de las Darknets.

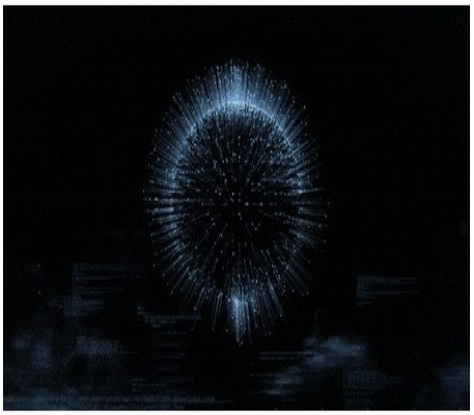
La Surface Web es el Internet que conoces.

El primero de los conceptos que tienes que conocer es el de la 'Clearnet' o 'Surface Net', términos que en castellano significan 'Red Limpia' o 'Red de superficie'. Ambos se refieren a lo mismo, **Internet tal cual lo conocen la mayoría de los cibernautas**, ese pedazo de la World Wide Web a la que cualquiera puede acceder fácilmente desde cualquier navegador.

Se trata de una red en la que somos fácilmente rastreables a través de nuestra IP. La componen principalmente las páginas indexadas por los buscadores convencionales como Google, Bing o Yahoo, pero también **todas esas otras webs a las que puedes acceder de forma pública** aún sin estar indexadas, como puede ser Facebook, Twitter y demás redes sociales, así como cualquier otra página web o blog.

Es difícil saber su tamaño exacto. Según Internet Live Stats esta está compuesta por más de 1.139 millones de páginas web, mientras que datos como WorldWideWebSize.com apuntan a que las superficie de Internet cuenta con más de 4.700 millones de páginas indexadas. Sea como fuere, la red accesible sigue teniendo sólo una pequeña parte de los datos que navegan por el ciberespacio.

Deep Web, las profundidades de la World Wide Web.



Así como en líneas generales la Clearnet es esa porción de Internet a la que puedes acceder fácilmente con tu navegador, podríamos decir que **la Deep Web viene a ser justo lo contrario**. Teniendo en cuenta que el ~90% del contenido de la red no es accesible a través de motores de búsqueda estándar, estamos hablando de muchos datos. También conocida como Invisible Web (Web Invisble) o Hidden Web (Web Oculta), engloba toda esa información que está online, pero **a la que no puedes acceder de forma pública**. Por una parte, pueden tratarse de páginas convencionales que han sido protegidas por un paywall, pero también archivos guardados en Dropbox o correos electrónicos guardados en los servidores de nuestro proveedor. a Deep Web también la componen sitios con un "Disallow" en el archivo robots.txt o **páginas dinámicas que se generan al consultar una base de datos**. Por ejemplo, cuando entras en un portal de viaje y buscas un hotel en una ciudad determinada para un día concreto, la página que se crea con los resultados se indexa en ningún buscador, es temporal y forma parte de la Deep Web

Dark Web, el Internet de las profundidades.

Muchas veces confundida con la Deep Web, aunque forma parte de ella, la Dark Web es ese fragmento de Internet al que sólo se puede acceder mediante aplicaciones específicas. Así como la Deep Web supone en torno al 90% de del contenido de la World Wide Web, **la Dark Web ocuparía únicamente el 0,1% de ella**.

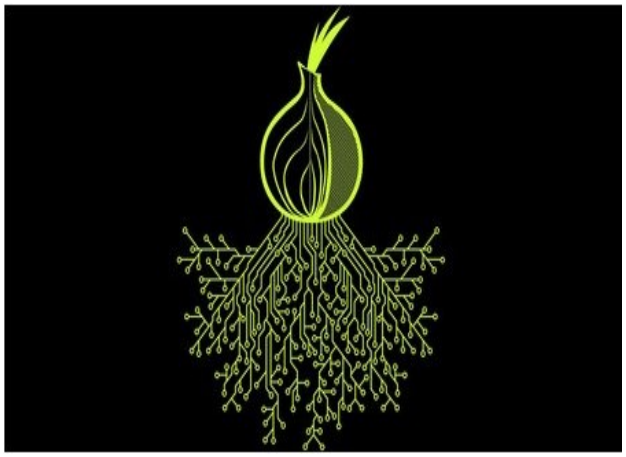
Páginas como Diccionary.com la definen como "la porción de Internet que **está intencionalmente oculta a los motores de búsqueda**, usa direcciones IP enmascaradas y es accesible sólo con un navegador web especial: parte de la Deep Web". Por lo tanto, aunque ambas están ocultas de los buscadores convencionales, la Deep Web es una recopilación de todo lo que hay fuera de ellos, incluyendo la Dark Web, que forma parte de ella pero es algo diferente.

Principalmente la Dark Web suele formarse por páginas que tienen dominios propios como las .onion de TOR o las .i2p de los eepsites de I2P, pero **a las que no puedes acceder a no ser que tengas el software necesario** para navegar por las Darknets en las que se alojan.

Existe la creencia de que, como la Deep Web suele ser en cierta manera la parte de Internet no indexada por los buscadores comerciales, la Dark Web no puede ser indexada por ninguno. Pero esto no es del todo cierto. Vale, en Google no encontrarás acceso a ella, pero **existen otros buscadores específicos** en los que sí que se puede hacer.

Algunos son accesibles desde la Clearnet, como Onion City, capaces de indexar miles de páginas .onion. También existen **otros buscadores dentro de las propias Darknets** como not Evil, Torch o una versión de DuckDuckGo también hacen lo mismo. Además, otras herramientas como Onion.to permiten acceder a las Dark Webs de TOR con sólo añadir la terminación *.to*, al dominio *.onion*, de manera que la web luzca como *tupagina.onion.to*.

Darknets, las redes independientes que componen la Dark Web.



El término Darknet fue acuñado en 2002 en el documento "The Darknet and the Future of Content Distribution" escrito por Peter Biddle, Paul England, Marcus Peinado y Bryan Willman, cuatro investigadores de Microsoft. En él se refieren a ella como **una colección de redes y tecnologías** que podría suponer una revolución a la hora de compartir contenido digital.

Para explicar este concepto podríamos decir que mientras la Dark Web es todo ese contenido deliberadamente oculto que nos encontramos en Internet, **las darknets son esas redes específicas como TOR o I2P** que alojan esas páginas. Vamos, que aunque Internet sólo hay uno, la World Wide Web, hay diferentes darknets en sus profundidades ocultando el contenido que compone la Dark Web.

Las más conocidas son la red friend-to-friend Freenet, I2P o Invisible Internet Project con sus Eepsites con extensión .i2p o ZeroNet. con sus múltiples servicios. **Pero la más popular de todas es TOR**, una red de anonimización que tiene también su propia Darknet, y es básicamente a la que suele referirse todo el mundo cuando habla de ellas.

Teniendo en cuenta que no hay una definición prestablecida para las Darknets, tienes que tener en cuenta que aunque técnicamente es algo diferente, en muchas ocasiones **se suele utilizar este mismo nombre para referirse a la Dark Web**. O sea que no te asustes si ves en los medios que se refieren a uno como lo otro, lo importante es que se sepa diferenciar por fin de la Deep Web.Pero esta imagen que tienes arriba te marca la diferencia, mostrándote que la Darknet son las redes ocultas en sí, mientras que **Dark Web se puede utilizar para referirse dos cosas**. Por una parte, el término se utiliza para referirse al contenido, a las webs oscuras, mientras que por otra también se usa para hablar de la cultura que implica, un concepto un poco ambiguo para referirnos a todo lo relacionado, y que tantas veces se confunde con Deep Web.

Las connotaciones negativas de la Darknet.

Darknet, red oscura, traducido el nombre enseguida te das cuenta de que puede tener una connotación negativa. Esto no es así por casualidad, ya que muchas de las Dark Webs que suele haber alojadas en ellas suelen tener fines negativos. Asesinos a sueldo, anonimato total y habitaciones rojas, **no todos estos mitos son reales**, pero ya vimos que no son pocas las páginas en las que encontrar objetos, sustancias o contenidos de dudosa legalidad. Sin embargo **no todo el mundo acepta estas connotaciones negativas**, y muchos piensan en el término "oscuro" de estas redes como un símil de algo que está oculto entre las sombras. No porque sea necesariamente negativo, ya sabemos que en las Darknets también

Ataques al DNS: cómo intentan dirigirte a páginas falsas.

A pesar de ser algo esencial para el correcto funcionamiento de Internet tal y como lo conocemos actualmente, los servidores DNS suelen pasar **desapercibidos** para la mayoría de los usuarios. Al menos así es hasta que ocurre algún tipo de ataque o incidente que afecta a su correcto funcionamiento y comprueban en primera persona cómo los servicios que utilizan todos los días comienzan a fallar, algo que pudimos ver no hace mucho cuando la botnet Mirai atacó a la empresa DynDNS.

Lo cierto es que hay más de un tipo de ataque que podría afectar a estos servidores; en este artículo veremos las diferencias entre ellos.

¿Qué es un servidor DNS?

El sistema de nombres de dominio (o DNS por sus siglas en inglés) es lo que nos permite **resolver el nombre de una página web por su dirección IP**. De esta forma, los usuarios no debemos acordarnos de la secuencia de números que conforman una IP (o números y letras en IPV6) y podemos acceder, por ejemplo, a una web como "www.facebook.com" escribiéndola tal cual en nuestro navegador, en lugar de escribir "31.13.92.36".

De resolver cuál es este nombre entendible para los usuarios en una dirección IP se encargan los servidores DNS, basándose en una base de datos distribuida y jerárquica que almacena a qué dirección IP corresponde cada nombre de dominio, entre otras funciones. De esta forma, es más fácil acordarse de las direcciones web, además de que la dirección IP puede cambiar por varias razones.

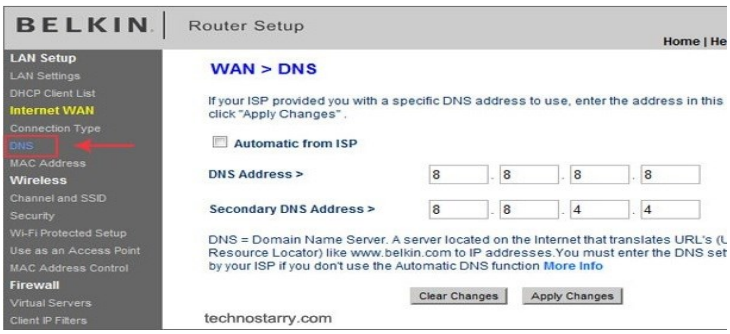
DNS Spoofing vs. DNS Cache Poisoning.

Muchas veces interpretados como si fueran el mismo tipo de ataque, la realidad es que, técnicamente, existen diferencias entre estos dos. En líneas generales, podríamos decir que el de DNS Cache Poisoning es una de las **múltiples formas** de conseguir un DNS Spoofing, refiriéndose este último a la amplia variedad de ataques existentes que buscan suplantar la información que se almacena en los servidores DNS.

DNS SPOOFING REFIERE A LA AMPLIA VARIEDAD DE ATAQUES QUE BUSCAN SUPLANTAR LA INFORMACIÓN ALMACENADA EN LOS SERVIDORES DNS

El DNS Spoofing representaría la finalidad última del ataque (conseguir **modificar los registros** que se almacenan en el servidor DNS por los que decida el atacante) y para la cual se emplean diferentes mecanismos. Entre ellos, encontramos el DNS Cache Poisoning, pero también ataques Man-In-The-Middle, uso de estaciones base falsas o incluso comprometer la seguridad de un servidor DNS.

También es posible que veamos cómo se hace referencia al DNS Spoofing cuando hablamos de ataques orientados al usuario. Un ejemplo de esto sería la **suplantación de la dirección** de los servidores DNS configurados en nuestro sistema operativo o router. Lo normal es que se introduzca la dirección de los DNS de nuestro proveedor de Internet u otros como los de Google, tal y como vemos a continuación:



En lo que respecta al DNS Cache Poisoning, se refiere a la situación en la que muchos usuarios finales utilizan la misma cache donde se almacenan los registros que relacionan cada dirección IP con un dominio. En el caso de que un atacante consiguiera manipular una entrada DNS en ese registro, los proveedores de Internet que utilizan esa cache lo tomarían como auténtico, por mucho que haya sido **manipulado para dirigir a una web fraudulenta.**

UNA CACHE DNS ENVENENADA NO REDIRIGE CORRECTAMENTE A LAS IP LEGÍTIMAS CUANDO RESUELVE UN NOMBRE DE DOMINIO

Uno de los principales problemas de los ataques de DNS Cache Poisoning es que se pueden propagar entre varios servidores DNS, afectando con el tiempo **también a los routers domésticos** e incluso a la cache DNS existente en el sistema del usuario, ya que recibirían esta información incorrecta y actualizarían su cache local con ella. Para realizar este tipo de ataque se necesita disponer de un servidor web y de un servidor DNS, configurando su propio DNS autoritativo y un dominio trampa. A partir de ahí, el atacante debe primero conseguir que la víctima acceda con su propio DNS al enlace con el dominio trampa, para así empezar a recolectar los identificadores de transacción hasta que sea capaz de **predecir** cual será el siguiente.