Dominios .Onion

Castaño Apaza Guery
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
ryguer_j@hotmail.com

RESUMEN

Mediante el siguiente artículo daremos a conocer acerca del dominio .onion ya que muchos no lo deben conocer, porque comúnmente navegamos por el primer nivel dentro de la Deep Web, así veremos cómo se utiliza, para qué nos puede servir y como tener un sitio web en TOR, ya que el dominio .onion al igual que Tor es muy importante al ingreso al internet profunda.

Palabras Clave

Web, dominio, información, seguridad, anonimato.

1 INTRODUCCION

Los dominios .onion actúan como dominios de alto nivel tipo las .com o las .org, pero no son accesibles como una página normal. Por esa razón se las llama casi dominios. Las .onion corren a través de la red TOR. El tor no solo encripta los datos sino que incrementa el anonimato. En la web normal, una página de contenido ilegal puede ser dada de baja por el gobierno del país en donde se encuentra el servidor. Pero con la red TOR, no solo es imposible decir en qué sitio está el servidor sino que también es casi imposible derribarlos.

2 ¿QUE SON LOS DOMINIOS .ONION?

Es un pseudo dominio de nivel superior genérico que indica una dirección IP anónima accesible por medio de la red Tor.

Las direcciones son resultado de una combinación de 16 caracteres alfanuméricos generados sistemáticamente basándose en una clave pública cuando Tor es configurado. Esa combinación de 16 caracteres puede ser creada con cualquier letra del alfabeto y con dígitos decimales que empiecen por 2 y acaben en 7 representando así un número de 80-bit en base 32.

Forman parte de la Deep Web. Aunque tales direcciones no son en realidad DNS, los buscadores web pueden acceder a sitios .onion usando proxy y enviando la solicitud a través de servidores de la red Tor. El objetivo de usar este sistema es hacer que tanto el distribuidor de información como el receptor sean difícilmente trazables, ya sea entre ellos, o por un tercero. En la web de la "superficie" podemos hacer un seguimiento, o encontrar webs por medio de buscadores. En la Deep Web no hay buscadores, (sólo algunos facilitadores), el usuario debe conocer la web que va a visitar, muchas veces bajo contraseña. En la Deep Web se puede encontrar el

contenido de la web tradicional pero también todo aquello que no aparece en la ella.

Ejemplo:

En el siguiente sitio .onion se puede encontrar información sobre esta red: <http://am4wuhz3zifexz5u.onion/> pero para ingresar se debe tener TOR instalado o bien utilizar un proxy web como Tor2Web e ingresar al siguiente enlace: <https://am4wuhz3zifexz5u.tor2web.org/>

El OnionRouting, fue introducido por David M. Goldschlag, Michael Reed y Paul Syverson aplicando las ideas de David Chaum para conseguir redes que preserven la privacidad y anonimato (tanto del mensaje como los interlocutores) de forma transparente a las entidades que se comunican. Los mensajes son repetidamente cifrados e enviados a través de varios nodos y redes (onionrouters) y cada nodo elimina la información del nodo anterior, previniendo que se conozca la información de origen/destino y el contenido del mensaje.

En esta red alternativa, las direcciones de las páginas no tienen el formato habitual y son casi ilegibles e imposibles de recordar, empiezan por HTTP (no dejan de ser páginas Web) y tienen la terminación .ONION. Para poder acceder a la Deep Web es indispensable estar conectado a la red Tor y utilizar un navegador Web como Tor Project que dispone de versiones para Windows, Linux y Mac.

2.1 ¿Que contiene las .onion que no se encuentren en la Web?

- Todo tipo de Pornografía
- Terrorismo
- Trata de Personas
- Hacking
- Tutoriales sobre armas, bombas, drogas etc.
- Venta de órganos
- Pedofilia
- Sicarios
- Compra de artículos robados
- Activismo (AnonymousWikileaks etc.)
- Códigos Fuentes de programas
- Cracks, Seriales, Keygens
- Virus, Malware y muchas cosas más.

La mayor parte de las transacciones en las .onion son llevadas a cabo mediante las Bitcoins. Puedes comprar virtualmente cualquier cosa con esta moneda. De todas formas, se cuestiona si sigue siendo anónimo. (1 Bitcoin > \$14 dólares).

Ejemplos de sitios .onion

Los siguientes sitios son accesibles a través de la red Tor:

- Core.onion, mítico portal de inicio en la web de onions.
- InspecTor / ExcludeNodesgenerator, ficha de mantenimiento de nodos falsos.
- Torchnetworksearch, índice y motor de búsqueda.
- La biblioteca Tor, pequeña biblioteca de libros en PDF y otros formatos comunes.
- Talk.masked, tablón de post anónimos.
- TorStatusNet, StatusNet en Tor (similar a Twitter).
- FreedomHosting, alojamiento gratuito para webs ocultas con PHP y MySQL.

En octubre de 2011, el colectivo hacktivista Anonymous hizo caer los servidores de FreedomHosting como parte de la operación OpDarknet, una campaña contra la pornografía infantil.² Anonymous denunció ante la prensa que FreedomHosting se había negado a eliminar sitios como "Lolita City" y "Hard Candy", los cuales se descubrió contenían 100 GB de pornografía infantil. Anonymous publicó 1500 nombres de usuario de esos sitios e invitó al FBI y a la Interpol a investigarlos.

3 COMO INSTALAR TU PROPIO DOMINIO .ONION Y TENER TÚ SITIO WEB EN TOR

Con las nuevas revelaciones del espionaje de USA en el mundo por parte de la NSA que vulnera los derechos de las personas con la excusa de la seguridad de los ciudadanos de Estados Unidos (por que la seguridad de otras naciones les importa un comino), cada vez es más importante que tengamos cuidado de nuestra propia privacidad, de que utilicemos herramientas y comunicaciones más seguras para evitar ser víctimas de este tipo de abusos por cualquier gobierno, ya sea el propio o uno extranjero. Una de esas herramientas es TOR, un protocolo de comunicaciones que permite navegar la llamada deep web y donde es casi imposible que alguien pueda identificarte y saber que buscas, que navegas o que transmites por medio de esta red.

TOR utilizar una peculiar forma de acceder "páginas web" mediante los llamados dominios .onion que son dominios como lo que conocemos por ejemplo www.google.com, pero estos dominios solo son accesibles utilizando la red TOR. Una de las ventajas es que al usar estos dominios, nunca conoces a que IP te conectas ni el servidor sabe desde que IP accedes para ver la información. Por esto creo que es importante que cualquier persona sepa como instalar un servidor Debian e instalar un servidor web que sea accesible por medio de un

dominio .onion para publicar un sitio web en la red TOR y así aumentar el nivel de privacidad y anonimato.

Conocer esto creo que nos da 2 ventajas: la primera podremos publicar información en internet de forma privada y anónima cuando lo creamos conveniente, la segunda apoyaremos a generar más contenido en la red TOR, y que no solo se use para buscar temas censurados o ilegales, sino que podremos, al igual que en internet, encontrar cualquier cosa que busquemos pero de forma privada y anónima. En pocas palabras, mas contenido = mas usuarios = mayor velocidad de uso en TOR.

4 CONCLUSION

Como pudimos ver los con los dominios .onion se pueden encontrar variedad de páginas, con contenidos ya sean fuertes y peligrosas dentro de la internet, pero se debe tener mucho cuidado al navegar dentro de esta, por el mismo que hay mucha delincuencia y policías informáticos.

La ventaja de usar los dominios .onion es para investigaciones para colegios y universidades, que permiten entrar a paginas que nos bloquean del internet normal.

5 BIBLIOGRAFIA

[1] <http://www.rn.org/docs/162798.pdf>

[2] <http://www.vebelio.taringa.net/posts/info/12971987/Red-onion-la-subred-dentro-de-la-internet.html>

[3] <http://www.omicrono.com/2013/08/tor-la-red-anonima-de-internet-sufre-el-peor-ataque-de-su-historia-por-parte-de-los-eeuu/>

[4] <http://www.comoinstalarlinux.com/como-instalar-tu-propio-dominio-onion-y-tener-tu-sitio-web-en-tor/>

[5] <http://www.taringa.net/posts/info/12971987/Red-onion-la-subred-dentro-de-la-internet.html>