¿Está roto el anonimato de Tor?

Molleapaza Calamani Marina
Universidad Mayor de San Andrés
Facultad de Ciencias Puras y Naturales
Carrera de Informática
mmolleapaza@ymail.com

RESUMEN

El anonimato es una red de Tor compuesta por túneles virtuales que permite a los usuarios mejorar su privacidad en Internet. Los usuarios pueden utilizar Tor para evitar que las webs los rastreen a la vez que permite conectarse a páginas web y otros servicios online que estén bloqueados por sus proveedores de Internet locales, todo ello sin necesidad de revelar su ubicación.

Palabras clave

Anonimato, Seguridad, The Onion, Router, Cibercrimen.

1. INTRODUCCION

Durante años TOR, (The Onion Router) ha sido el programa más popular que permite navegar en internet de manera anónima. Es una de las piezas fundamentales de lo que se conoce como Deep Web lleva tiempo siendo objetivo de los gobiernos y empresas que buscan conocer quién es quién y dónde está cada servidor dentro de esta red.

Fue creada originalmente por el Laboratorio de Investigación Naval de EE.UU. y la utiliza la gente que quiere enviar información a través de Internet sin ser rastreada. Esta red es utilizada por los periodistas y los funcionarios encargados de hacer cumplir la ley, pero también se ha vinculado a la actividad ilegal, incluyendo tráfico de drogas y la venta de imágenes de abuso infantil.

Y es por esa razón hacen muchos ataques sobre la red con el objetivo de acabar con el anonimato, y que además se han puesto en práctica.Los portavoces de la red de TOR admiten que el anonimato fue puesto en peligro.

De acuerdo con el comunicado el ataque del sistema comenzó el 30 de enero de 2014 y se percataron de él el 4 de julio de ese mismo año. De manera que los usuarios que hayan usado TOR en ese lapso podrían haber expuesto su identidad.

Figura 1. Descarga de Tor

2. EL ATAQUE A TOR

El ataque a esta red se llevó a cabo entre comienzos de febrero hasta el pasado 4 de julio. Al parecer ciertos *relays* maliciosos tenían como objetivo **"des-anonimizar" a los usuarios** de servicios ocultos, y aunque esos *relays* ya fueron purgados, hay *una brecha de cinco meses*, además de varias cosas por determinar, incluyendo el tipo y la cantidad de información que obtuvieron los atacantes

Los encargados de la red revelaron la existencia de una maniobra basada en la modificación de los encabezados del protocolo de Tor, para realizar lo que se conoce como *"ataque de confirmación de tráfico"*, combinado con un *"ataque Sybil"* que falsifica identidades.

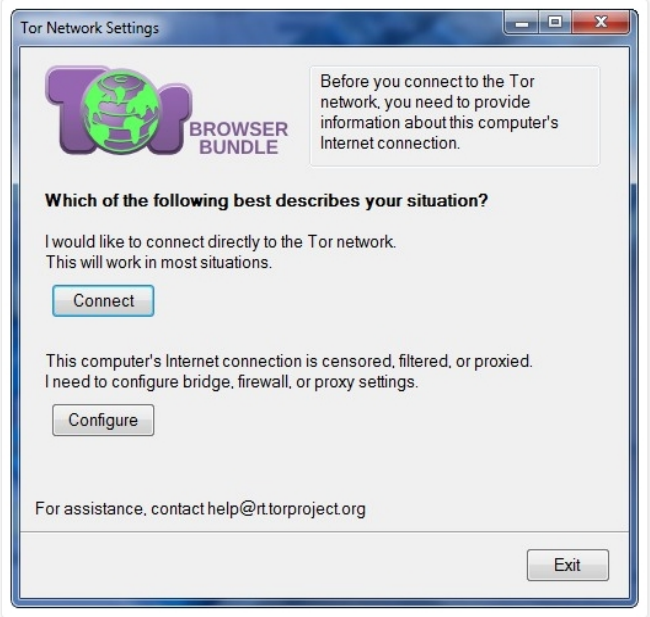

Figura 2. Conectandose con Tor

Un ataque de confirmación de tráfico trabaja *controlando los relays* en ambos extremos de un circuito Tor. Una vez que el volumen del tráfico, el tiempo, y otros aspectos son comparados, se puede concluir si ambos relays están dentro del mismo circuito. Cuando el primer relays del circuito conoce la dirección IP del usuario, y el último relays establece la ubicación del recurso al que se desea acceder, el usuario en cuestión queda efectivamente "des-anonimizado".

De hecho las agencias de investigación usan agentes infiltrados para llegar personalmente a los ciberdelincuentes que manejan esta red para fine ilicitos, porque el rastreo de IPs no los lleva a su blanco.

Por otra parte, otro incentivo para acabar con TOR puede provenir de Rusia, donde Vladimir Putin ofrece 100, 000 dólares a quien obtenga los datos protegidos por el sistema.

3. ANALIZANDO LA VULNERABILIDAD

Como se ha descubierto una grave vulnerabilidad se encontraron 115 nodos intermedios de la red Tor que estaban actuando de forma maliciosa lo que representa alrededor de un 6.4% del total de usuarios de esta red.

Mediante la utilización de esta vulnerabilidad recientemente descubierta de ataques de confirmación de tráfico. Esto significa que si un atacante dispone de un número elevado de nodos comprometidos se podría introducir un marcador en cada uno de los paquetes que se envíen y calcular, dependiendo de cuando se observa ese paquete en otro nodo, que paquetes han ido pasando por los mismos nodos.

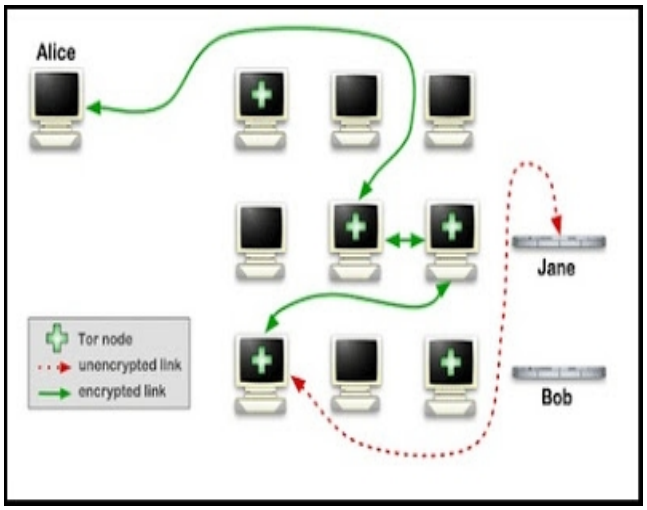

Figura 3. Funcionamiento de Tor.

No se sabe cuántos datos han recogido los atacantes y, debido a la forma en que el ataque se ha desarrollado, las modificaciones de su protocolo.

Todavía no está claro cómo fueron afectados los usuarios y hasta qué punto han descubierto las verdaderas identidades.

4. CINCO MESES VULNERABLES

Según el comunicado publicado por los desarrolladores de Tor, los nodos maliciosos se incorporaron a la red Tor el pasado 30 de enero de 2014 y fueron eliminados el 4 de julio, dejando una ventana de 5 meses durante la cual pudieron estar realizando este ataque y asumiendo que todos los usuarios que utilizaron la red durante ese periodo podrían haberse visto afectados.

Con seis meses de captura de tráfico sería posible saber las rutas seguidas por los paquetes, los servidores utilizados y su ubicación con un margen de acierto del 80%, según se deduce del estudio ”Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries“.

Según se ha sabido, los nodos maliciosos han estado utilizando las versiones 50.7.0.0/16 ó 204.45.0.0/16 durante los 5 meses que duró el ataque. Cuando se descubrió la vulnerabilidad se actualizaron estas versiones a la 0.2.4.23 ó 0.2.5.6-alpha para así cerrar el agujero de seguridad. No obstante, el uso de ataques de confirmación de tráfico sigue suponiendo una amenaza para asegurar la privacidad de la red.

5. LA AGENCIA DE SEGURIDAD NACIONAL

Algunos espías cibernéticos del Gobierno estadounidense y el británico filtran deliberadamente información sobre las vulnerabilidades de la llamada 'red oscura' que vigilan, según un gerente de Tor Project.

Andrew Lewman, director ejecutivo de Tor Project, empleados de la Agencia de Seguridad Nacional (NSA) de EE.UU. y del Cuartel General de Comunicaciones del Gobierno del Reino Unido (GCHQ) filtran detalles sobre los 'agujeros ' que encuentran en su código. Ello permite a los programadores de Tor corregir las imperfecciones.

La NSA consiguió identificar a varios usuarios y acceder a sus computadores.

Una técnica desarrollada por la NSA tuvo como objetivo el navegador Firefox utilizado con Tor, lo que dio a la agencia control total sobre estos ordenadores, como el acceso a los archivos, todas las pulsaciones de teclado y todas las actividades en Internet, haciendo referencia a unos de los materiales que en su día entregó Edward Snowden al periodista Glenn Greenwald, quien lo acaba de hacer público.

6. REFERENCES

[1] http://satelitemedia.mx/tor-es-atacado-y-el-anonimato-esta-en-peligro/

[2] http://www.elladodelmal.com/2014/07/tor-confirma-que-el-anonimato-se-rompio.html

[3] http://rsclick.es/2014/08/04/la-red-tor-deep-web-atacada-para-desanonimizar-usuarios/

[4] http://www.elladodelmal.com/2013/09/como-ser-anonimo-en-internet-la-red-tor.html

[5] http://actualidad.rt.com/actualidad/view/137971-nsa-gchq-filtran-datos-agujeros-red-anonima-tor

[6] http://actualidad.rt.com/actualidad/view/107520-tor-nsa-espionaje-red-anonima-eeuu