Vulnerabilidades en el explorador TOR

Lilian Paola Fuentes Caro / *lilian.fuentes1@correo.icesi.edu.co*
Bryan Camilo Grueso Gomez/*bryan.camilo.grueso@correo.icesi.edu.co*
Beycker Alexis Ágredo Mosquera/*beycker.agredo@correo.icesi.edu.co*

Universidad Icesi, Cali-Colombia

Abstract-

In the last years the topic of the privacity on the internet make the users consider about using other ways to hide the information that they consume, download, search and share. One of this ways is Tor. Tor is a tool that encrypt the information and erase the traffic of the user on the internet, but not at all. In this paper, will be show about how safe is Tor and if there is any vulnerability in this tool.

I. Introducción

El presente trabajo investigativo pretende indagar superficialmente las vulnerabilidades encontradas en el explorador Tor en los últimos años. Sin embargo, a medida que se van encontrando falencias en el explorador que pudieran exponer el anonimato de la red, estas son parchadas; haciendo que TOR sea un explorador "confiable" en el cual los usuarios pueden navegar sabiendo que no están comprometiendo su información de red a terceros. Si bien, en aspectos técnicos y bajo las configuraciones adecuadas el explorador demuestra ser eficiente en temas de seguridad, existen muchas técnicas usadas por la NSA que rompen el anonimato de los usuarios. El siguiente proyecto se enfocará en técnicas basadas en señuelos para atrapar ciberdelincuentes. Además, se hará una demostración de una técnica muy utilizada que si bien no rompe las seguridad de Tor, se aprovecha de la infraestructura de Tor creando señuelos de páginas que cierto tipo de gente suele visitar para robar información personal, ya sea a través de scripts usando Javascript o creando descargables que engañen al usuario.

II. Hipótesis

La realización de este proyecto se fundamentó bajo la siguiente interrogante: ¿ Es posible interceptar a un usuario de la red Tor?

III. Objetivos

A. Objetivo General

Plantear un escenario en la red TOR, en el cual se pueda rastrear a un cibercriminal a través de un hosting web señuelo publicada en la Deep web.

B. Objetivos Alcanzables

1. Explicar cómo se podría romper el anonimato de un usuario dentro de la red TOR.
2. Montar una página señuelo en la red onion.
3. Implementar código en java que permita detectar la información de red de un individuo.

C. Objetivos No Alcanzables

1. Insertar un enlace en el sitio web que le permita al criminal descargar e instalar el archivo en java.

IV. DESARROLLO

"The Onion Router (TOR) es un explorador web gratuito, que usa una red abierta con la finalidad de permitir a las personas mejorar su privacidad y seguridad en la Internet. La herramienta permite que los usuarios de la red no tengan que preocuparse por el rastreo de sus datos por parte de alguna agencia gubernamental del país". [1]

La forma en como TOR permite mantener ocultos a los usuarios en la red es haciendo que los paquetes "reboten" de un servidor a otro, encapsulando la información en cada uno de los tres routers elegidos para la conexión a Internet. Cada vez que se realiza una petición a algún servicio en Internet, dos de los tres routers mencionados anteriormente cambian en el circuito, haciendo que sea muy difícil de rastrear un paquete desde su origen al destino, y en caso de ser rastreado, el paquete aun cuenta con el triple cifrado característico de la red Onion. Pero internamente ¿cómo interactúan los nodos entre sí? Como se menciona en [2] cada nodo sólo tiene información de la capa superior e inferior a la propia, sin tener acceso a información de las otras capas las cuales podrían ser el destino o el origen. Adicionalmente, todos los datos que viajan por la red están cifrados de manera que ningún nodo podrá saber la ruta completa de la conexión. Para finalizar el recorrido de los paquetes de datos, el último nodo solamente recibe una petición desde el nodo anterior, ignorando el circuito por completo, para completar esta solicitud; el último nodo es el único que conocerá el destino hacia dónde se dirige la información.

Si bien el explorador ha demostrado ser una herramienta confiable para los usuarios que desean mantener la privacidad de sus conexiones a Internet, la tecnología no es perfecta y TOR no es la excepción a la regla.

“El 10 de septiembre de 2018, Zerodium, una plataforma de compra y venta de exploits y vulnerabilidades, publicó en su perfil de Twitter que detectó una vulnerabilidad Día Cero en el navegador que permitía saltarse las medidas de protección a través de una puerta trasera, lo que permitiría ejecutar código malicioso de forma remota”.[3]

La vulnerabilidad fue detectada en la versión 7 del navegador TOR; no obstante, dicho fallo de seguridad fue parchado en la versión 8. La manera en cómo operaba el fallo era configurando el “Content-Type” de una web como “text/html/json”, de esta manera se podría insertar código malicioso en el explorador pudiendo quebrantar la confidencialidad de los usuarios de la red.

Investigadores de la firma italiana de ciberseguridad “We Are Segment” divulgaron el hallazgo de una falla crítica en el navegador TOR que revela la dirección IP real de los usuarios. La vulnerabilidad recibe el nombre de TorMoil y afecta a usuarios de Mac y Linux. El fallo se activa aprovechando un error de software de Firefox, el navegador en el cual está basado TOR. El usuario accede a un enlace cuya dirección comienza con file:// en lugar de http:// o https://. Una vez alguien, que ha sido infectado por la vulnerabilidad, navega por un sitio web diseñado especialmente para capturar la IP, el sistema operativo puede conectarse directamente al host remoto pasando por alto el navegador TOR. Es en ese momento en el que se puede conocer la IP real de donde se está conectando el usuario y no la que proporciona el navegador para evadir el seguimiento. Al igual que en el fallo anterior, esta vulnerabilidad fue parchada en la actualización posterior del explorador.

Cada vez que se halla una vulnerabilidad que implique una brecha en el software de TOR, los desarrolladores del navegador lo parchan tan pronto algún usuario lo reporta. No obstante, aún existen puertas traseras que permiten conocer la identidad de un usuario en la web, estos al no ser errores de software no hay una forma de mitigarlos por completo. La mayoría de las técnicas usadas para conocer el origen de un paquete en la red TOR, son utilizadas por agencias de ciberseguridad para detectar cibercriminales en la Darknet.

La NSA (National Security Agency) y otras organizaciones como la CIA son los principales causantes de que muchas personas desconfíen de la seguridad de TOR, ya que no tienen garantía del nivel de anonimato que les pueda brindar este navegador. E-mails, mensajería instantánea (como el chat de Facebook) y hasta el historial de navegación de millones de personas podrían ser revisado por la NSA. En la actualidad existen muchas tácticas empleadas por la NSA para monitorear con detalle la actividad de los ciudadanos en Internet. Según The Guardian, la agencia cuenta con un sistema llamado XKeyscore, que le permite a analistas buscar sin autorización previa en bases de datos de e-mails, mensajería instantánea (como el chat de Facebook) y hasta el historial de navegación de millones de personas. Cubre "casi todo lo que un usuario típico hace en Internet", asegura el documento filtrado por Edward Snowden [5]. No obstante, las autoridades estadounidenses niegan tales afirmaciones.

Aunque no se ha podido ratificar los alcances del software de la NSA, si se conoce que la agencia cuenta con personal especializados en técnicas basadas en engañar a los cibercriminales de la red. “La principal vulnerabilidad descubierta por la NSA está relacionada con Adobe Flash. El plugin de Adobe Flash del navegador crea un canal de comunicación dedicado hacia el servidor y se puede capturar la dirección IP real del cliente, por lo que el usuario estará totalmente desenmascarado” [4]. Los desarrolladores de TOR Browser actuaron en consecuencia a esa vulnerabilidad, lo que los llevó a excluir Flash del navegador con el fin de proteger a los usuarios. A pesar de ello, la NSA ha usado frecuentemente esta vulnerabilidad para atrapar a delincuentes en la red, incitando mediante anzuelos a que los cibercriminales (especialmente pederastas) instalen el plugin en el explorador pese a las medidas de seguridad impuestas por los desarrolladores. De esta forma, la NSA ha tenido éxito en muchas de sus operaciones, por ejemplo, interviniendo webs de pornografía infantil alojadas en la Darknet.

V. Resultados

Para la realización de la parte práctica, se utilizó un software llamado WampServer. Dicho software consta de una pila de software para el sistema operativo Microsoft Windows. Este software consta de un servidor web Apache, OpenSSL para el soporte de SSL, bases de datos como MySQL y programación web de PHP. Con el servidor configurado, se utiliza el recurso de Tor llamado “torrc” el cual se configura para generar en el archivo host name la URL pública del servidor; con esto, cualquiera que pertenezca a la red onion podrá ingresar a la página señuelo si tiene la URL.
Para crear el URL, Tor crea el servicio oculto generando el nombre aleatorio mediante una clave RSA de 1024 bits y luego calcula el SHA-1 utilizando un pedazo de la clave pública. Este es un proceso complejo que luego dará como resultado un nombre aleatorio y cifrado para nuestro sitio web.

IMAGEN 1
ENTORNO DE DESARROLLO WAMP

Durante la elaboración del proyecto se realizó una pagina web señuelo con el fin de demostrar que pese a las buenas medidas de seguridad de Tor, no significa que esté protegido frente a las páginas que interceptan las direcciones IP con el fin de rastrear su información.

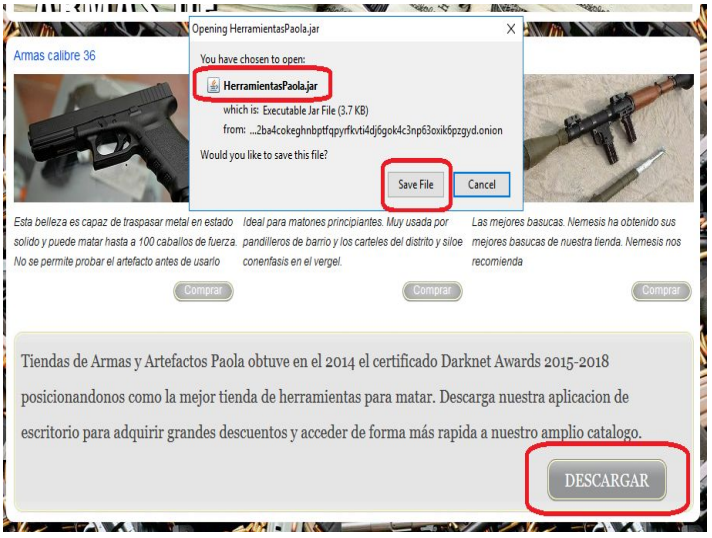

IMAGEN 2
PÁGINA SEÑUELO

La página web de la Imagen 2 muestra un enlace para obtener una aplicación del sitio web que proporciona descuentos en la compra de armas si se descarga de dicha aplicación de escritorio.

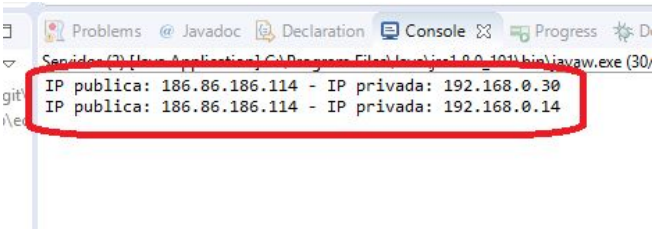

IMAGEN 3
ENTORNO DE DESARROLLO PARA EL EJECUTABLE

En la Imagen 3, se muestra los datos que se envían al eclipse debido a que el programa es un señuelo que al ser ejecutado manda automáticamente la dirección IP pública y privada de quien lo abrió. Ya con esta información se puede hacer un rastreo y obtener más información del usuario que la utiliza.

VI. CONCLUSIÓN

TOR es el navegador más seguro conocido hasta ahora para navegar en la Deep Web y la Darknet. Su sistema de seguridad y de encriptación son fiables, sin embargo, siempre habrán vulnerabilidades que se puedan explotar, debido a que ningún sistema es totalmente seguro a causa de que los errores humanos siempre estarán presentes, más en específico por parte de los usuarios finales, que es el sector más atacado para poder obtener información y credenciales del mismo.

Las fallas más conocidas por TOR se deben a errores humanos o a manipulación de terceros con un alto grado de conocimientos en Hacking, como lo es la NSA, por lo que, siempre están monitoreando a las personas, sobre todo aquellas que quieren navegar anonimamente; trayendo como consecuencias ataques masivos a la seguridad de TOR para poder acceder a los usuarios que consumen dicho servicio.

Tor al ser una gran red de servidores y usuarios onion que no se conocen entre sí se puede crear páginas señuelo con el fin de robar información haciéndose pasar por un usuario mas del monton, lo que dificulta encontrar al culpable del robo de la información, haciendo que la misma seguridad y anonimato que brinda tor sea una gran ventaja para la persona que hurta los datos de los clientes que caen presa de su sitio web.

REFERENCIAS

[1] HDCO, “11 cosas que debes y no debes hacer con Tor”, [documento online], 2014. Disponible: https://blog.hostdime.com.co/11-cosas-que-debes-y-no-debes-hacer-con-tor/

[2] Anónimo, “Cómo funciona la red Tor?”, [documento online], 2018. Disponible: https://tor.derechosdigitales.org/torificate/p1.2/

[3] José García Nieto, “Descubren una vulnerabilidad Zero Day en el navegador Tor y la revelan porque ya no ganarán dinero con ella”, [documento online], 2018. Disponible: https://www.genbeta.com/actualidad/descubren-vulnerabilidad-zero-day-navegador-tor-revelan-porque-no-ganaran-dinero-ella

[4] Yubal FM, “Adobe Flash y Metasploit, así identificó el FBI a usuarios de la red TOR”, [documento online], 2018. Disponible: https://www.genbeta.com/actualidad/adobe-flash-y-metasploit-asi-identifico-el-fbi-a-usuarios-de-la-red-tor

[5] Cony Sturm, “XKeyscore, el programa de la NSA que recolecta 'casi todo' lo que se hace en Internet”, [documento online], 2013. Disponible: https://www.fayerwayer.com/2013/07/xkeyscore-el-programa-de-la-nsa-que-recolecta-casi-todo-lo-que-se-hace-en-internet/