Cómo la NSA intenta espiar a los usuarios de Tor

N GENBETA :: 07/10/2013

'The Guardian' sigue con las filtraciones de la NSA, y la última se refiere a Tor, software que permite navegar de forma anónima y acceder a servidores web ocultos

Todo con tráfico cifrado y enrutado de tal forma que es muy difícil detectar la procedencia original.

Tor está basado en la técnica del enrutado cebolla o por capas. A grandes rasgos, lo que hace el cliente es enviar un paquete a un nodo de la red, este lo envía a un segundo nodo, el segundo a un tercero… y así siguiendo una ruta más o menos aleatoria hasta que sale de la red Tor, llega a Internet y la respuesta vuelve al cliente original. Todo ello con cifrado a cada paso: tenéis una explicación más completa de cómo funciona Tor en Genbeta.

La NSA y el GCHQ han utilizado ataques conocidos junto con su poder e influencia para "desanonimizar" a usuarios de Tor. Sin embargo, no lo han conseguido con el 100% de usuarios ni han logrado atacar a usuarios específicos: por el contrario, lo que hacen es "poner trampas" y ver quién cae. Tampoco han roto la seguridad y cifrado de Tor, los ataques se dirigen más bien a otros programas que use el objetivo para "colarse" en su ordenador.

Lo que la NSA ha hecho con Tor se puede dividir en dos partes: por una, análisis para detectar a los usuarios y por otra ataques para comprometer sus ordenadores y poder espiarles sin problemas de forma continuada.

Análisis: desde usuarios "tontos" hasta revelación de cookies

La NSA quiere saber quién está haciendo qué en Internet en todo momento, y Tor se lo pone difícil. Todas las técnicas de análisis están enfocadas a saber quién está detrás de cada petición de Tor, para o bien añadir esos datos a sus registros o bien efectuar más ataques sobre el objetivo posteriormente.

La primera parte consiste en distinguir si una petición a una página web viene de la red Tor o de un usuario normal. No es un paso difícil: Tor deja muchas huellas que hace que su detección sea sencilla. Por ejemplo, TorButton no desvela el número de compilación de Firefox que estás usando. Lo hace por motivos de privacidad, y porque no pasa nada si se detecta una petición Tor: lo que de verdad importa es que no se pueda distinguir entre varios usuarios Tor.

Lo siguiente que hay que hacer es saber quién hay detrás, y la NSA ha desarrollado varias técnicas de análisis.

En las presentación filtrada por 'The Guardian', la que más me ha llamado la atención es 'Dumb users' (EPICFAIL), o en castellano "Usuarios idiotas (fallo épico)". La idea es sencilla: fijarnos en fallos de los usuarios que revelen su identidad. Por ejemplo, pongamos que un

usuario, Bob, escribe normalmente en un foro bajo el seudónimo bob8819. Más tarde, empieza a usar Tor para visitar otras páginas. La NSA no sabe quién es el que está haciendo esas visitas, hasta que de repente Bob escribe en su foro habitual bajo su seudónimo de siempre usando Tor. Con esa información, Bob ha desvelado su identidad y ha permitido a la NSA vincular esas visitas desconocidas de Tor con otras visitas de las que ya conocía el origen.

En resumen, lo que hace la NSA es vincular el tráfico de un usuario Tor a otro tráfico normal (que sabemos de dónde viene) mirando qué partes comunes hay entre los dos. Aquí, las partes comunes eran nombres de usuario y correos.

El siguiente nivel es usar las cookies. La idea es aprovechar cookies que “sobrevivan” a la navegación con Tor, por ejemplo si se usa mal el navegador con Tor y no se borran al pasar a la navegación normal (no anónima). Según la presentación, las cookies de 'DoubleClick' (red de anuncios) serían una buena forma para identificar usuarios Tor.

Por último, la NSA también podría estudiar la fecha, hora y lugar de conexión de un objetivo y después buscar conexiones a Tor con los mismos parámetros. Sin embargo, es difícil seleccionar los candidatos y los programas que están en marcha no son muy eficaces.

Estudiar la red Tor para descubrir a los usuarios originales

El otro tipo de técnicas de análisis se basan en estudiar la red Tor. La primera es sencilla de entender: la reconstrucción de circuitos. Si la NSA controla todos los nodos de un circuito, podría vigilar por dónde va el paquete, desde que lo envía el usuario original hasta que sale a Internet. Sin embargo, controlan un número muy bajo de nodos, de tal forma que la probabilidad de que un paquete visite sólo los nodos de la NSA es ínfima, lo que hace la reconstrucción de circuitos casi imposible.

También existe el análisis de tiempos, que es igualmente simple. Por ejemplo, pueden detectar que cuando un paquete entra a la red Tor, sale otro a los 300 milisegundos en otra parte del mundo hacia el ordenador de nuestro amigo Bob. Si se repite mucho ese patrón de latencia, es muy posible que ese tráfico de Tor esté originado por Bob.

Exploits, ataques directos contra usuarios: FoxAcid

Una vez que la NSA ha detectado quién está detrás de un cierto tráfico Tor, pasa a atacarle para ganar acceso a su ordenador y poder espiarle continuamente.

Los ataques se ejecutan de varias formas. Muchas veces, se atacan vulnerabilidades en Firefox (el navegador usado por Tor Browser Bundle). Por ejemplo, Egotistical Giraffe aprovechaba un fallo en la gestión que Firefox hacía de la librería EX4. También se cree que podrían haber explotado una vulnerabilidad en Javascript. Tampoco era fácil de hacer, ya que muchas veces los usuarios de Tor desactivan Flash y JavaScript y por lo tanto exponen menos vulnerabilidades.

Los encargados de explotar estas vulnerabilidades (entre otras muchas) son los servidores FoxAcid. Estos servidores tienen un nombre de dominio normal, son públicos y no parecen

tener relación con la NSA. Cuando los visitas no son más que otra página web más, normal y corriente.

Esos servidores responden sólo a URLs especiales, llamadas etiquetas FoxAcid. Cuando un navegador visita una URL especial, el servidor infecta el navegador y después el ordenador entero para poder controlarlo.

Esa URL, además de decir a FoxAcid que hay que atacar al visitante, también contiene una identificación que permite al servidor saber a quién está atacando, qué relevancia tiene, si es un objetivo prioritario… ¿De qué le sirve saberlo?

Como imaginaréis, no es una buena idea que el usuario pueda detectar que está siendo atacado. Por eso, en función de su importancia, FoxAcid utiliza unas u otras vulnerabilidades. Por ejemplo, para un objetivo muy importante explota las vulnerabilidades más potentes y difíciles de detectar y menos usadas, para garantizar que el ataque tendría éxito. Si, por el contrario, el objetivo no es tan importante, usarían vulnerabilidades más conocidas para evitar ser detectados y también para no desvelar su "artillería pesada".

La identificación también sirve al grupo TAO (Tailored Access Operations) para especificar los planes de ataque a cada objetivo. Una vez infectado el objetivo, se ejecutan varios "programas" en su ordenador. Entre ellos, los más básicos recogen información y configuraciones del ordenador para transmitirlos a la NSA y permitir así a un analista infectar todavía más el ordenador y llevar a cabo otro tipo de tareas.

¿Cómo llevar al usuario a FoxAcid? Quantum

No hemos explicado cómo conseguía la NSA que los usuarios visitasen los servidores de FoxAcid. Usaban técnicas como el phishing, o modificando páginas web visitadas por sus objetivos (por ejemplo, un foro de discusión sobre marxismo); incluso a pesar de que eso podría infectar a cualquier usuario de Tor, entre los que hay informantes de EEUU o personal de su ejército.

Sin embargo, lo más importante es el programa Quantum. Quantum responde más rápido que el servidor legítimo para que el objetivo reciba las respuestas deseadas.

Los servidores Quantum llevaban a cabo ataques 'man-in-the-middle', o de "hombre en el medio". El método de ejecutarlos es bastante burdo. Cuando un usuario hace una petición a un servidor, Quantum lo detecta y responde al usuario antes de que le llegue la respuesta del servidor legítimo. Tal y como están diseñados los protocolos de red, el ordenador del usuario se quedará con la respuesta de Quantum y descarta la del servidor legítimo por haber llegado más tarde.

Para que estos ataques tengan éxito, la NSA se aprovecha de su poder y acuerdos con las telecos. Los servidores Quantum están en puntos centrales de la red de Internet, de tal forma que serán mucho más rápidos que cualquier otro servidor.

Con Quantum, la NSA puede modificar la respuesta que recibe el usuario y hacer lo que quiera con ella. Por ejemplo, puede decirle que la dirección de descarga de una imagen de

una web es la de un servidor de FoxAcid, lo que desencadenará un ataque cuando el navegador trate de mostrar la imagen.

'Exploits' para que el usuario se descubra

Con FoxAcid la mayoría de ataques son dirigidos, pero también existe la posibilidad de llevar a cabo ataques más generales (por ejemplo, como comentábamos antes, modificando páginas web que suelan visitar los objetivos). En este caso, la NSA seguiría sin saber quién es el usuario real, así que han creado 'exploits' que hagan que el ordenador descubra su identidad.

Por ejemplo, podrían marcar el tráfico saliente o el 'user-agent' (la cadena que identifica el navegador) para poder seguir los paquetes cuando salgan de la red Tor. También podrían forzar a los usuarios a usar circuitos que sólo pasen por nodos controlados por la NSA.

Tor sigue siendo seguro, pero usarlo quizás te ponga en peligro

La NSA todavía no ha conseguido romper Tor ni su cifrado. No puede coger un paquete de tráfico Tor y decir automáticamente de dónde viene y qué datos tiene. De hecho, las técnicas que usan no son especialmente efectivas ahora mismo, sobre todo si el usuario toma las precauciones necesarias. De hecho, tanta técnica nos indica que no hay ninguna puerta trasera y que podemos confiar en Tor a pesar de que lo financie el Departamento de Defensa de EEUU.

Tampoco parece que quieran tumbar Tor. Ya no porque les resulte difícil, sino porque muchos de sus objetivos lo usan y asustarlos podría ser contraproductivo.

El problema ahora mismo es precisamente ese: usar Tor te pone en el punto de mira. Puedes ser víctima de un ataque de la NSA que infecte tu ordenador sin que te des cuenta. Como nos comentaban hace unos días, si la NSA quiere, puede entrar y no vas a poder detectarlo.

La solución sería usar Tor pero tomando precauciones, sobre todo las que recomienda la propia gente de Tor: https://www.torproject.org/download/download-easy.html#warning

genbeta.com. Revisado por La Haine

---

https://www.lahaine.org/mundo.php/como-la-nsa-intenta-espiar-a-los-usuario