Dos investigadores de seguridad informática han demostrado una técnica para interceptar tráfico en forma casi indetectable. La técnica, del tipo man-in-the-middle , utiliza el protocolo BGP para desviar tráfico en cualquier lugar del mundo hacia la estación de monitorización y luego lo envía (posiblemente modificado) hacia su destino.

Peter Zatko, uno de los investigadores, declaró: *"Es un problema enorme. Es un problema al menos tan grande como el de DNS , si no más grande"*
. Peter Zatko es un ex miembro del grupo L0pht y en 1998 testificó ante el congreso estadounidense diciendo que podría detener totalmente Internet en 30 minutos utilizando un ataque BGP similar. También instruyó a agencias de inteligencia sobre la posible utilización de BGP para monitorizar tráfico remoto sin necesidad de colaboración por parte de ningún ISP...

La técnica descrita intercepta el tráfico por dirección de destino, y no siempre es posible desviar tráfico que ocurre dentro de un mismo ISP. El protocolo BGP mantiene tablas de rutas para encontrar la más eficiente hacia un destino dado. Pero las rutas están basadas en las máscaras de red y la más restrictiva (la más específica) gana. Para interceptar el tráfico, todo lo que tiene que hacer un atacante es publicar un rango de IPs más pequeño que el que está publicado por su legítimo dueño. La publicación se propaga en minutos a todo el mundo y el atacante comenzará a recibir datos destinados a los rangos IPs publicados.

Si sólo se hiciera esto, sería muy fácilmente detectable ya que el tráfico "desaparecería" hacia otra red en vez de llegar a su destino. Esto es más o menos lo que pasó este año cuando un ISP de Pakistán desvió por error todo el tráfico de YouTube (en realidad el tráfico *hacia* YouTube) hacia direcciones inexistentes. Obviamente todo el mundo se dio cuenta.

Lo innovador de la técnica presentada es la capacidad de poder redirigir el tráfico hacia su destino final después de ser interceptado, algo que normalmente no sería posible ya que las tablas BGP harían que el tráfico volviese al atacante. Sin embargo, se utiliza otra capacidad del protocolo BGP llamada "AS path prepending", que permite seleccionar algunos routers para que no acepten la publicación BGP maliciosa hecha por el atacante y lograr de ese modo que tengan las tablas BGP originales. Luego es cosa de enviar el tráfico por medio de éstos routers y llegará correctamente a destino.

Si los datos siempre llegan a destino correctamente, ¿quién va a notar algo?

En todo el proceso **no se aprovecha ninguna vulnerabilidad**, ningún fallo del protocolo, ningún error de software. Simplemente se saca provecho a la arquitectura BGP que está basada en la confianza mutua.

Anton Kapela, el otro investigador, dijo que los ISP pueden evitar este tipo de ataques utilizando filtros. El problema es que se requiere una gran cantidad de filtros y trabajar en coordinación con todos los otros ISPs. También tendría un alto costo de mantenimiento. Por todo esto, Kapela opina que una solución basada en filtrado no va a prosperar.

Otra solución propuesta se basa en la autenticación de los "dueños" de los bloques IPs. Una solución de éste tipo requeriría la utilización de certificados por parte de los ISPs. Sin embargo, aunque se evitaría el desvío de tráfico en el primer salto en una ruta, lo que evitaría desvíos

accidentales como el de Pakistán, este esquema no evitaría el desvío del segundo o tercer salto en una ruta.

Stephen Kent y sus colegas de BBN Technologies, han desarrollado Secure BGP (SBGP), que requiere que cada router BGP firme digitalmente todas sus rutas publicadas con una clave privada. Esto evitaría totalmente el desvío malintencionado de tráfico, pero lamentablemente los routers actuales no tienen ni la memoria ni la capacidad de procesamiento para generar y validar firmas, por lo que una implementación masiva de SBGP requeriría el cambio a gran escala de todos los routers involucrados, algo que ni los ISP ni los fabricantes de routers se ven motivados a hacer por ahora.

Fuente: kriptópolis , wired