

Ataques DDoS basados en JavaScript

by javier - Jueves, junio 11, 2015

<http://memoriasdeunsysadmin.tk/2015/06/11/ataques-ddos-basados-en-javascript/>

Comencemos por el principio

Quiero empezar este artículo con una breve explicación sobre ataques DoS. Para los que no estén en el tema, un ataque DoS (Denegación de servicio) busca normalmente saturar un servidor o una red de modo que esta esté demasiado ocupada y no sea capaz de atender peticiones legítimas. Hay muchas variantes y formas. En los últimos tiempos, una de estas variantes se ha convertido en una auténtica pesadilla.

DDoS

Los DDoS, o ataques de Denegación de Servicio distribuidos se caracterizan por no provenir de una sola fuente. De este modo alcanzan tamaños monstruosos y se hacen más difíciles de bloquear o evadir. Para lograr estos ataques, normalmente se usan vulnerabilidades en equipos diversos alrededor del mundo, o bien se los infecta con algún tipo de malware. De este modo y, sin sospecharlo, miles y millones de equipos se convierten en atacantes. Sin entrar mucho en profundidad aún, una de las cosas que hace más difícil la defensa contra estos ataques, es que al tratarse de equipos incluso domésticos, con IPs dinámicas, no conviene bloquearlas. Ello implicaría bloquear usuarios reales NO-infectados mañana o pasado.

JavaScript y los DDoS

JavaScript es una tecnología difundida mundialmente que permite añadir muchas funcionalidades a un sitio, incluida la interactividad, recurso crítico hoy en día para lograr atraer usuarios y "lealtad" por su parte. El código javascript puede agregarse directamente en el html o bien puede cargarse desde un sitio remoto. El hecho de poder cargar contenido en un sitio, sin necesidad de seguir links y cargar nuevas páginas, supuso un gran avance. Sin embargo, el que un javascript pueda hacer llamados a https es a la vez muy útil y muy peligroso.

Ejemplo de ataque

Por ejemplo, supongamos que en un sitio A se incluye un script que carga una imagen de un sitio remoto B. Un pequeño detalle, la imagen se llama 1000 veces por segundo. Con esto, cada visitante al sitio A, sin saberlo, está participando de un ataque DDoS masivo al sitio B. cuyo servidor podría fácilmente saturarse y ser incapaz de servir peticiones "legítimas". Si el sitio A tiene una cierta cantidad de visitas o, incluso, si en lugar de un solo sitio "atacante" A, hubieran varios A1, A2, A3, esto podría tener dimensiones interesantes. Si los sitios atacantees, son específicamente creados por el atacante, es probable que no sean sitios populares y con muchas visitas. Sin embargo, podría también pasar que un sitio con muchas visitas sea comprometido y este código inyectado en su código original. Esto no es tan difícil como uno podría pensar y hay miles de sitios comprometidos por día. Algunos incluso, siguen comprometidos sin saberlo por días y a veces semanas.

Librerías JavaScript comprometidas

Otro caso muy común, es el de los sitios que usan librerías javascript alojadas en un servidor externo. De acuerdo a reportes de CloudFlare(empresa con vasta experiencia filtrando ataques de este tipo, son muchos los sitios construídos usando librerías javascript comunes de terceros, tales como JQuery, Facebook SDK y GoogleAnalytics.

Si una de esas librerías se viera comprometida con código que realice un ataque, los visitantes de todas las páginas que implementen dicha librería se convertirían instantáneamente en parte de un DDoS probablemente mundial. Esto también puede parecer algo difícil de que ocurra, sin embargo, CloudFlare informa que esto ya ha sucedido: JQuery.com, que sirve la librería JavaScript más usada actualmente, fue comprometido en el 2014.

Aún hay más

Por si esto fuera poco, se encontró otra manera de llevar a cabo este tipo de ataques, ya que los compromisos a nivel servidor generalmente son detectados pronto y rápidamente corregidos. Una manera más compleja aún de hacer que visitantes a un sitio ejecuten código malicioso es a través de los ataques Man in the middle(Hombre en el medio). En este "mecanismo" el atacante busca ponerse en el medio entre clientes y servidor(visitantes y sitio), de manera de poder hacerse pasar por el segundo y responder "en su nombre". Ve y recibe las solicitudes de los visitantes y los puede transmitir al servidor, aprovechando para espiar la solicitud y/o alterar la antes de mandar la respuesta al visitante.

Volviendo a los ejemplos anteriores, cuando un sitio llama a un javascript remoto, un atacante en el medio puede muy fácilmente devolver un javascript adulterado conteniendo código malicioso.

También podemos imaginar qué sucede si un atacante logra suplantar un ISP, ya que tendría la posibilidad de inyectar código malicioso a infinidad de sitios, aunque, claro está, este no sería el peor escenario de una intrusión a tal nivel.

Conclusión:

La mejor manera de proteger nuestro sitio de estos ataques es claramente el uso de certificados SSL. Mediante HTTPS se encripta el tráfico, de modo que no se pueda leer ni alterar. Un certificado también es un modo eficiente de garantizar identidad, por lo que complica a un atacante la suplantación de identidad.

Bibliografía:

[Introducción a Ataques DDoS basados en JavaScript](#)(En inglés, blog de CloudFlare)

[Jquery.com comprometido](#). Nota de Riskiq(En inglés)

[Un ataque DDoS basado en Javascript, visto por SafeBrowsing](#)(En inglés)

memoriasdeunsysadmin.tk