https://info.nodo50.org/Ataque-informatico-contra-Nodo50.html

Ataque informático contra Nodo50

- Noticias - Noticias Destacadas -

Fecha de publicación en línea: MiÃ©rcoles 21 de diciembre de 2011

Entre las 20 hs. y las 24 hs. del miércoles 21 de diciembre se produjo un ataque contra uno de nuestros servidores. Consistía en el envío de un flujo enorme de tráfico contra una de nuestras IPs, cientos de miles de paquetes UDP por segundo. A pesar de bloquear a las IPs atacantes en nuestro router perimetral, el enorme tráfico de paquetes de datos generado por el ataque afectó a la capacidad de la infraestructura de conexión a Internet de nuestro rack (armario de servidores). Entre las 20 y las 23 hs. se produjo una pérdida de parte de los paquetes de conexiones legítimas y eso hizo que todos los servicios fueran lentos.

A partir de las 23 hs. la situación se normalizó. Y a las 24 hs. el ataque cesó.

Nos parece importante dejar claro que no se ha producido ninguna intrusión ni robo o destrucción de datos. El ataque consistía en saturar la infraestructura de red con una inundación de tráfico basura.

La compra de un router, que realizamos al mudar nuestros servidores a Suecia en julio pasado, ha resultado una buena inversión. Con él pudimos, entre las 21 y las 23 hs., mitigar los efectos del ataque y por lo menos era posible acceder al correo web o descargar lentamente páginas web. También nos vino bien tener una entrada de administración secundaria a los servidores, los que nos permitía trabajar en ellos para mitigar el ataque sin que el propio ataque nos lo impidiera. Son dos cosas que en el centro de datos de Amsterdam no teníamos.

Este tipo de ataque busca saturar la infraestructura de red superando su capacidad de procesamiento de paquetes. No se trata de saturar con el volumen de datos, así que el tamaño del ataque no se mide en MB/sg si no en paquetes/sg. Precisamente los paquetes eran muy pequeños, de 60 bytes (en vez de los 1500 habituales en muchos protocolos) para poder generar muchos en poco tiempo. El ataque llegó a los 300.000 paquetes por segundo, cuando lo habitual a esa hora pueden ser entre 500 y 3000.

Una cosa que pasa con este tipo de ataques es que no hay pistas sobre su autoría. Cuando alguien ataca una web y consigue modificar sus contenidos suele dejar pistas sobre sus motivaciones (ideológicas, monetarias o de satisfacción de su ego). Pero cuando el ataque consiste en enviar paquetes de datos UDP cuyo contenido (quitando cabeceras, etc) es de 1 byte no se recibe ningún texto o imagen del atacante. Así que siendo honestos no podemos afirmar que haya sido un ataque de los adversarios ideológicos de Nodo50 y de las organizaciones que alojamos, ni que esté relacionado con el estreno de nuestro documental. Puede ser, pero no tenemos pruebas.

Siempre ocurre que de estas cosas se aprende, y ya estamos planeando mejoras en la infraestructura de red para tener mas opciones cuando se repita un ataque similar. Hay equipamiento especial para mitigar estos ataques, pero con precios a partir de 10.000 €, lo que excede ahora mismo nuestra capacidad económica. Pero hay alternativas mas económicas que vamos a estudiar. El uso que hacemos de la palabra "mitigar" no es casual, incluso con equipos que cuestan decenas de miles de euros sus fabricantes nunca prometen que podrán parar completamente los ataques, sólo garantizan la mitigación parcial de sus efectos.