**MEMCACHED**

Es un sistema distribuido para caché basado en memoria, libre y de código abierto, la última versión es del 7 julio 2018, programado en C.

Básicamente es un almacén clave-valor en memoria, para pequeños fragmentos de datos arbitrarios, por ejemplo, de resultados de llamadas a bases de datos, APIs etc.

Su propósito principal es mejorar la velocidad de las aplicaciones web al guardar en memoria diversos datos.

Hoy en día es usado por múltiples páginas web como YouTube, Reddit, Facebook…

Es originalmente una aplicación de Linux, pero también se puede usar en Windows, pero para ello se tiene que hacer uso de WAMP. Que seria como el análogo de LAMP pero en Windows.

Su arquitectura sigue un modelo cliente-servidor.

Los servidores son los encargados de mantener el almacén clave-valor y son los clientes los que acceden a él o añaden datos.

El cliente va a mantener una lista de todos los servidores, sin que estos se comuniquen entre sí. Cuando el cliente quiera acceder a algún servidor utilizará una librería. Dicha librería utilizará una función hash para realizar diversos cálculos y de esta manera seleccionar el servidor que va a interactuar con tabla hash que actúa como almacén clave-valor, una vez elegido el servidor inicia la comunicación con él, y luego este usará otra hash para determinar donde va a almacenar el valor en caso de que quiera guardar o de donde va a leer el dato deseado por el cliente.

Un dato importante que el cliente debe tener en cuenta cuando usa memcached es que precisamente como indica su nombre es una memoria caché, por lo tanto, cuando un servidor agota su memoria y necesita seguir incluyendo valores, elimina los mas antiguos. Por lo tanto puede darse el caso de que el dato no esté en esa caché cuando el cliente quiera acceder a él. Para intentar solucionar este problema se han inventado “MemcacheDB” y “Membase”. Membase es un sistema de gestión de bases de datos “NoSQL” simple, rápido y elástico. MemcacheDB es una alternativa a memcached que proporciona almacenamiento permanente.

Memcached, el ataque DDoS de moda

A pesar de que hasta ahora sólo hemos tratado ventajas también tiene inconvenientes bastante importantes, sobre todo relacionados con la seguridad, este mes de marzo se ha producido el ataque DDoS más potente de toda la historia dirigido hacia GitHub. Sin embargo pocos dias despues tambien se registró otro ataque que a pesar de que fue mitigado con rapidez, superó al anterior.

La frecuencia y la potencia de estos ataques se debe principalmente a que ya no requieren del uso de botnets sino que se aprovechan de la mal configuracion de miles de los servidores de Memcached que hay en internet. Los servidores de Memcached expuestos en la red carecen de cualquier protección ante autenticación con lo que cualquier ciberdelincuente puede acceder a ellos, y enviar una gran cantidad de datos con el objetivo de saturar los servidores y maximizar los índices de respuesta.

Los servidores Memcached pueden ser utilizados para la reflexión y amplificación de los ataques DDoS.

Pero, cómo funcionan estos ataques, bueno pues el primer paso es la reflexión. El atacante típicamente prepara un conjunto de servidores Memcached con pares clave-valor con una longitud arbitraria. Luego el atacante, o bien por si mismo o haciendo uso de una botnet, emite consultas Memcached para esos pares clave-valor, estas consultas son pequeñas (alrededor de unos 15 bytes) usando una dirección IP falsificada de un determinado servidor.

El siguiente paso es la amplificación, el servidor Memcached que ha sido comprometido responde con paquetes de una longitud mucho mayor (alrededor de unos 1442 bytes), es decir, la respuesta es amplificada relativamente al pequeño tamaño de los paquetes de las peticiones. Esta amplificación puede ser tan grande como multiplicar por 10000 el tamaño de las peticiones. Como las peticiones estaban usando una dirección IP falsificada, todo ese tráfico amplificado, se manda al servidor de destino. El resultado es la negación del servicio. La gran cantidad de tráfico supera al servidor y su ancho de banda.

MemcacheDB

Consta de un sistema operativo multiplataforma, y está escrito en “do”.

Como ya se dijo anteriormente, es una alternativa de persistencia habilitada de “memcached”. La principal diferencia con memcached es que tiene su propio sistema de base de datos clave-valor, esto nos indica que está destinado a un almacenamiento persistente en lugar de limitarse a una memoria caché no persistente.

Este sistema está basado en “Berkeley DB” que es una librería de software diseñada para proporcionar una base de datos integrada de alto rendimiento para datos clave - valor. Esta librería está escrita en el lenguaje C y es compatible con los lenguajes de programación más conocidos a nivel mundial como C#, C++, Java o Python, también está disponible en otros muchos lenguajes menos extendidos como Perl o Ruby.

Membase

También llamado “Servidor de CouchBase”, es un proyecto de código abierto, un paquete de software distribuido multi-modelo orientado a base de datos documental y optimizado para aplicaciones interactivas. Pueden servir a multitud de usuarios al mismo tiempo mediante la creación, almacenamiento, recuperación, agregación, manipulación y presentación de datos. Para soportar este tipo de necesidades, Couchbase Server está diseñado para proporcionar acceso a documentos de clave-valor o documentos JSON de fácil escala, con baja latencia y alto rendimiento sostenido.