Threat Bulletin

Memcached

June 2018

Memcached DDoS Attacks: Real-time Report

Memcached is free memory-caching software designed to speed up the operation of database-driven websites. Initially developed by American programmer Brad Fitzpatrick, the primary objective of this program was to employ unused server memory for file caching. Memcached is written in C and runs on Unix-like and Windows operating systems.

In February 2018, CloudFlare, a US content delivery and Internet security company, reported that several Memcached servers had been misconfigured and used to launch a series of Distributed Denial-of-Service (DDoS) attacks. The attacker used the Memcached protocol over User Datagram Protocol (UDP) to trick multiple Memcached servers into overloading the attack target by flooding it with data traffic. As a result, the target could not process legitimate requests and regular services came to a halt. This form of amplification attack is possible because the UDP network protocol enables the transmission of data without first receiving a "handshake", confirming the communication.

How Does It Work?

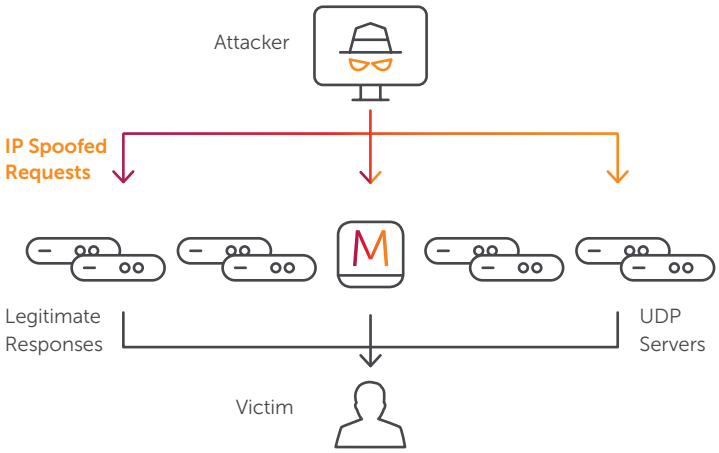
Memcached DDoS attacks are a type of UDP reflected amplification attack, which use vulnerable Memcached servers exposed on the Internet. First, the attacker loads the Memcached server database, and then it sends requests over UDP, using a forged IP address (the target's), to thousands of Memcached servers which are open on the Internet. The servers respond by sending many UDP packets coming from source port 11211 to the target.

In some cases, the volume of traffic can exceed one terabyte of data. Memcached is often used in social networks and is the program used to switch data back and forth between networks. As Memcached was never intended to operate across the public Internet, it has no authentication process built in. As such, it is easy to abuse and manipulate.

A Memcached attack operates similarly to all DDoS amplification attacks such as NTP and DNS amplification. The attack works by sending spoofed requests to a vulnerable server, which then responds with a larger amount of data than the initial request, magnifying the original volume of traffic. CloudFlare found that a 15-byte request could receive a response of 750 kB, or more than 50,000 times the original requested volume.

A Memcached attack occurs as follows:

1. A large amount of data is placed on an exposed Memcached server by an attacker.
2. The attacker fakes an HTTP GET request using the IP address of the target.
3. The Memcached server that receives the request then sends out a magnified response to the target.
4. The targeted server cannot process the large volume of data sent from the Memcached server, which overloads the targeted server resulting in a DoS to the legal requests.



Targets

Following a recent attack on Github, subsequent DDoS attacks have targeted both Google and Amazon, where the objective of the attacks was to totally knock the targets offline. Github suffered a 1.35 Tbps assault, to date, the largest DDoS attack on record, topping the record 1.2 Tbps Mirai attack. However, a subsequent attack on an unnamed US service provider experienced an attack measuring 1.7 Tbps. Most of the attacks have occurred in China and the US, with targets including the offices of Sony Interactive's Playstation and the gaming company Minecraft.net. Other targets included sites run by the US National Rifleman's Association and the Chinese-American newspaper, the Epoch times. So far, the instigators of these attacks have yet to be identified.

On a positive note, companies of the size of Google and Amazon are capable to withstanding the volumetric attacks due to their sheer absorption capacity. Smaller companies, without the infrastructure of these Internet giants are also finding that they can cope with the attacks considering that they arrive on a specific networking port. Chinese Internet security company, Qihoo 360 is currently transmitting real-time information on the ongoing assaults. So far, it has recorded over 15,000 attacks since they started in February 2018.

Protection

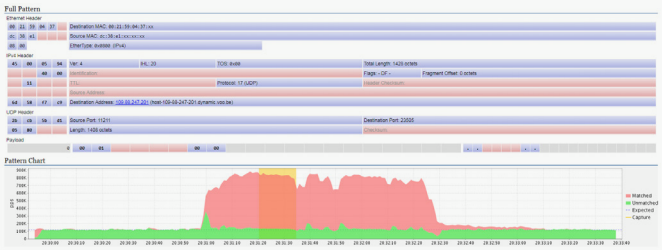
The principal measure to protect your Memcached servers involves disabling UDP support if it is not absolutely required. Additionally, Memcached servers can be insulated from the Internet by placing them behind a firewall. Another protective measure is to prevent the spoofing of IP addresses. However, this is a solution that can only be implemented by large server installations that have the capacity to prevent data packets from departing a network that originated from outside of that network. This means that ISPs must filter all traffic that leaves their networks to prevent it from being emulated on another network. Finally, another way to reduce the threat from such amplification attacks is to remove the amplification factor itself. If the response to a UDP request is always lower than the initial request then amplification would no longer be an issue.

To protect your network against Memcached attacks, further protective measures include:

- Where possible, ensuring that your servers are not accessible to the Internet.
- Installing at least one upstream provider so that in the event of an attack, you can resort to other links if the primary link is flooded.
- Establishing an anti-spoofing arrangement (such as BCP38 & 84) so that any spoofed packets, such as those used in DDoS reflection attacks are insulated from your network.
- Confirming that your networks deploy high performance, distributed, in-line packet inspection, which is capable of good traffic monitoring (both inbound and outbound).
- Employing machine-learning software that can detect and mitigate attacks at wire speed, regardless of scale, and within seconds of an attack taking place.

Attack pattern

Attack pattern and matched traffic reported by Allot's DDoS Secure management console



Further protection can be ensured by hardening your Memcached servers. This can be achieved by taking the following steps:

1. **Open /etc/memcached.conf** in a text editor
2. Locate the-m parameter
3. Change its value to at least 1 GB
4. Locate the-l parameter
5. Change its value to 127.0.0.1, or localhost
6. Save your changes to **memcached.conf** and exit the text editor
7. Restart your Memcached server

It is also highly recommended to close off port 11211. You should also consider deploying a DDoS mitigation services such as Allot's DDoS Secure. Other solutions such as transferring data to a scrubbing center have proved prohibitive for many CSPs and enterprises. Furthermore, short "hit and run" attacks are over too soon to be scrubbed.

Need a defense strategy against Memcached attacks?

We can help.

Contact Allot »