CO892 – Memcached DDoS Attacks Report

Bastien DHIVER – bfrd2 - 13/03/2018

1. Overview

On the 27th of February 2018, a new amplification vector has been clearly identified and used in the wild by attackers to perform volumetric attacks on various popular websites and infrastructures all over the Internet. A misconfiguration allowing the UDP protocol by default in the popular memory object caching software Memcached was the root cause. The attackers – whose identities remain unknown - targeted a wide range of victims such as the usual big players, the game industry, porn sites, security industry and political related websites. Some service outages were revealed.

Illustration 1: Memcached logo

2. What happened?

Memcached lack of authentication in the text protocol and the possible injections laid the basis to what the Chinese group of researchers from the cybersecurity Okee Team disclosed (slides copy) in June 2017. Since the 23rd of February 2018 a specific network traffic was detected by the Russian DDoS mitigation company Qrator Labs across entire Europe.

Memcached is a high-performance distributed memory object caching system. It is often used in speeding up dynamic web applications by having a fast access to data stored in RAM. The default configuration makes it listen on port TCP/11211 and UDP/11211 without any authentication and on every network interfaces. Memcached servers are in majority located in data centres with high-speed upstream transit links which makes them valuable assets for attackers.

The attack is classified as a UDP amplification/reflection attack that exploited misconfigured Memcached services exposed on the Internet. An **amplification attack** generates a response size that is much larger than the query size, meaning that a relatively low level of resources is required by an attacker to cause significant damages to the victim. A ratio exists between the size of the request and the "amplified" size of the response and is called the **amplification factor**. **Reflection attacks** spoof the incoming IP address of a request so that the response will be sent to the chosen host. The three-way TCP handshake does not exist in UDP, so spoofing is trivial.

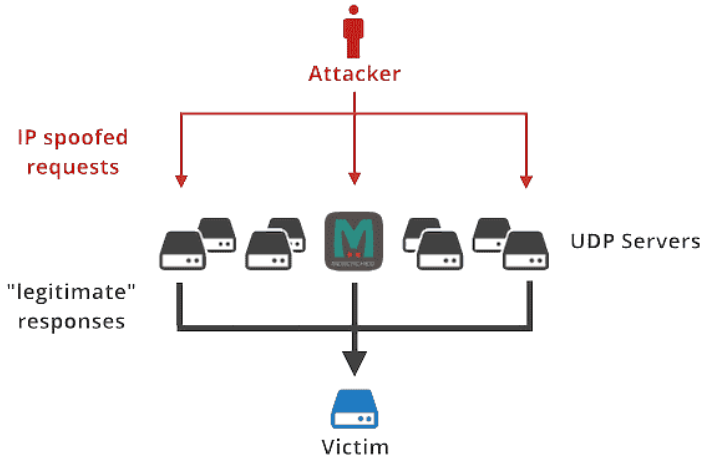

Illustration 2: Memcached DDoS attack scheme

Protocol	Bandwidth Amplification Factor
DNS	28 to 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5
Multicast DNS (mDNS)	2 to 10
RIPv1	131.24
Portmap (RPCbind)	7 to 28
LDAP	46 to 55
CLDAP [7]	56 to 70
TFTP [23]	60
Memcached [25]	10,000 to 51,000

Illustration 3: Protocols and their amplification factors

The basic attack flow goes as followed:

- A large payload is implanted by the attacker on the exposed Memcached server
- The attacker spoofs (reflection) a “get” request message with the target source IP
- A large response (amplification) is sent by Memcached to the specified IP

The amplification factor of Memcached is around 51,200 (and potentially more than 61,000+). That means that in practice, a 15 byte request result in a 750kB response. In comparison, the NTP service have an amplification factor of “only” 557. Observed packet size was about 1428 bytes. Part of that is that multiple keys or duplicated keys can be requested multiple times in a single request. Reflection techniques are not new and the proliferation of poorly secured IoT devices creates a dramatic growth in both, the number and the size of botnets such as the MIRAI botnet.

Up to 93,000 Memcached servers were listening on port 11211 on the 1st of March 2018, 600,000 were reported on November 2017.
The majority of vulnerable Memcached servers is concentrated in North America and Europe. They are hosted by major hosting providers such as OVH, DigitalOcean and Sakura Internet.

Several PoC, tools and exploits were developed very quickly in various programming languages and published all over the Internet.

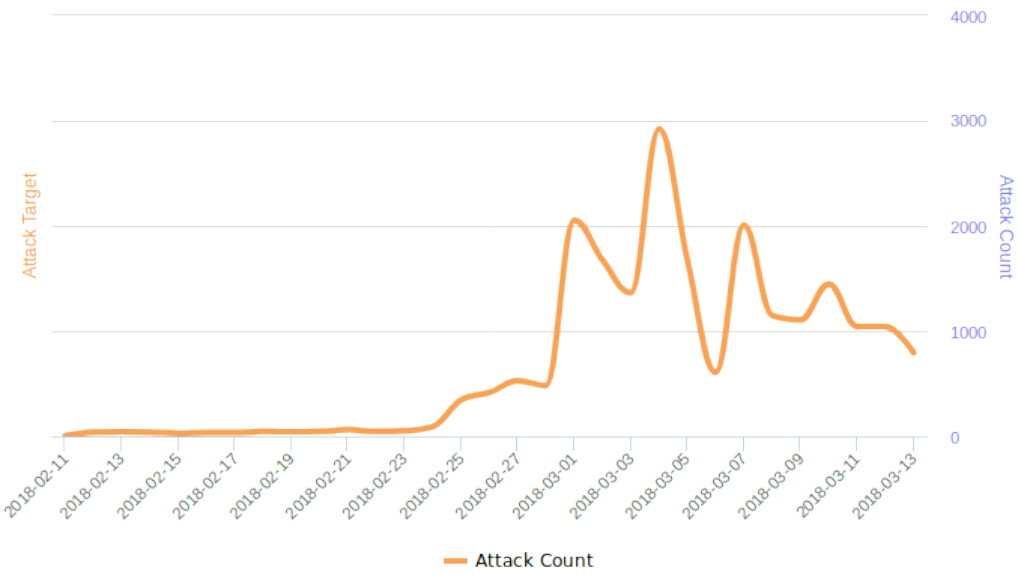

Illustration 4: Memcached reflection attack trends over the days

3. Impacts and consequences

The cached data is widely accessible without authentication and can be explored and corrupt but that is not new. Numerous tools/scripts exist to dump the content of caches such as this one which uses Shodan.io to find potential targets. Confidential database records, website customer information, emails, API data can potentially be found in caches.

GitHub.com service has been made unavailable for a couple of minutes on the 28th of February 2018 due to the usage of Memcached amplification used to conduct a huge DDoS attack. This attack peaked at 1.35Tbps. The network anomaly was detected by their monitoring and the incoming traffic was moved to Akamai who could provide additional edge network capacity and DDoS mitigation.

A client of the cloud company OVH was also targeted on the 1st of March 2018 with the same intensity of 1.3Tbps. The attack has been mitigated by OVH anti-DDoS VAC solution.

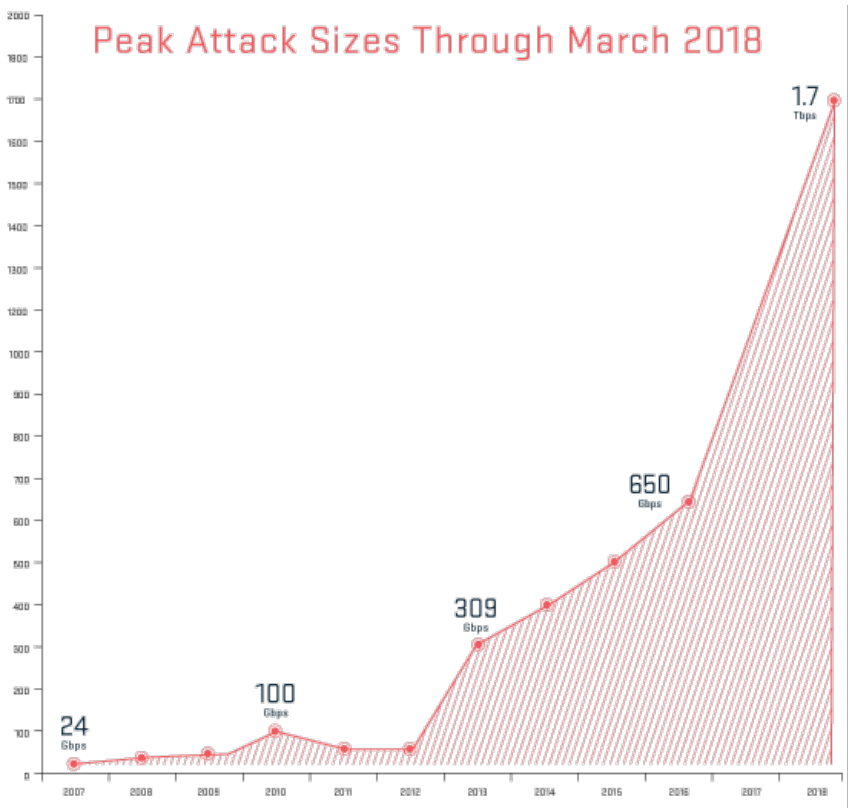

Illustration 5: DDoS traffic records over the years

The latest record-breaking was confirmed by Arbor Networks on the 5th of March 2018 and is about 1.7Tbps. This is the biggest volumetric DDoS attack ever publicly disclosed. The previous one was less than 1Tbps in 2016 and caused by the MIRAI botnet.

A list of targets is provided in a second Netlab 360 blog post: “Google, Amazon, QQ.com, 360.com, PlayStation, OVH Hosting, VirusTotal, Comodo, GitHub, Royal Bank, Minecraft and RockStar games, Avast, Kaspersky, PornHub, Epoch Times newspaper, and Pinterest”.

A ransom notes was repeatedly embedded in the implanted payload asking to pay 50 XMR (Monero) ~$16,000 to a specific wallet. Paying will not stop attacks from happening.

On the 7th of March 2018, Rapid7 noted a "substantial declined in exposed Memcached instances" that goes from 140,000 in 2017 to "only" 54,000 on the 6th of March, 2018. The CVE-2018-1000115 was assigned to the security issue and some GNU/Linux distributions have now changed the default Memcached configuration shipped within the package. A concern has been raised by the increasing number of probes on other ports used for amplification attacks and also the wide distribution of version exposed. Future attacks might be in preparations.

4. Detection and mitigation

Memcached UDP support must be disabled by users if not in use (the majority of the cases) and the service listening address/interface must be set carefully to the local host address/interface. A guide was made by OVH about it. Memcached server documentation reminds us to "not expose memcached directly to the internet". Version 1.5.6 fixes the issue.

Scanning the Internet for exposed Memcached listening in UDP is also possible… (and illegal) but you can scan your network IP address ranges:

```
masscan 0.0.0.0/0 -pU:11211 --banners | grep memcached
```

System/network administrators have to make sure that no Memcached servers are exposed to the Internet. A simple command can be used to test if a server is vulnerable (no output is expected):

```
echo -en "\x00\x00\x00\x00\x00\x01\x00\x00stats\r\n" | nc -q1 -u 127.0.0.1 11211
```

Nmap script and Metasploit script are also available to this extent. Watch for abnormally large responses to a particular IP address can be a first step to detect an amplification attack. Blocking port UDP/11211 via firewall rules, ACLs, or applying rate-limiting at peering/transit/customer aggregation edges can help to mitigate the issue. Corero Network Security have found a practical "kill switch" countermeasure. The DDoS victim can send back a simple command ("flush_all\r\n") in a loop to flush the content stored in cache of the server. However, this technique of "hack-back" is illegal in several countries. Tools available with shodan.io usage emerged.

Internet Service Providers (ISPs) must develop their interconnections with other networks (peering) to identify single points of failure in bandwidth usage and increase their robustness. Identifying internal IPs used as a reflector is also a good idea and can be the basis to apply a precise mitigation strategy. Having a good monitoring infrastructure is essential (the Chinese network security research lab NetLab 360 provide some), and should be coupled to internal flow analysis combined with external honeypots. Automation of intervention is a key factor. Implementing industry-standard Best Practices (BCPs) such as BCP38/84 is a must and helps to fight against a major IP network drawback which is IP spoofing. Cooperation is another key factor because attacks of this size cannot be easily defended against by data centre solutions. ISPs and cloud based DDoS protection services should work together to anticipate the threats and perform efficient mitigation as quickly as possible. Having a substantial network capacity or being "behind" a DDoS protection service can efficiently help to mitigate the effects of such attacks.

Developers are also concerned in order to prevent further attacks using the same vectors. Cloudflare urges developers to stop using the UDP protocol or not enable it by default. If UDP is used anyway, developers have to make sure that their applications will answer with a smaller packet size than the request and provide some sort of authentication. Vulnerable protocols must be fixed as soon as possible and the vulnerabilities be disclosed in a responsible manner.

More advices regarding generic UDP-Based Amplification Attacks Detection and Mitigation are given by US-CERT.