# Memcrashed - Major amplification attacks from UDP port 11211

By Marek Majkowski

Published: 2018-02-27 · Archived: 2026-04-05 13:48:19 UTC

2018-02-27

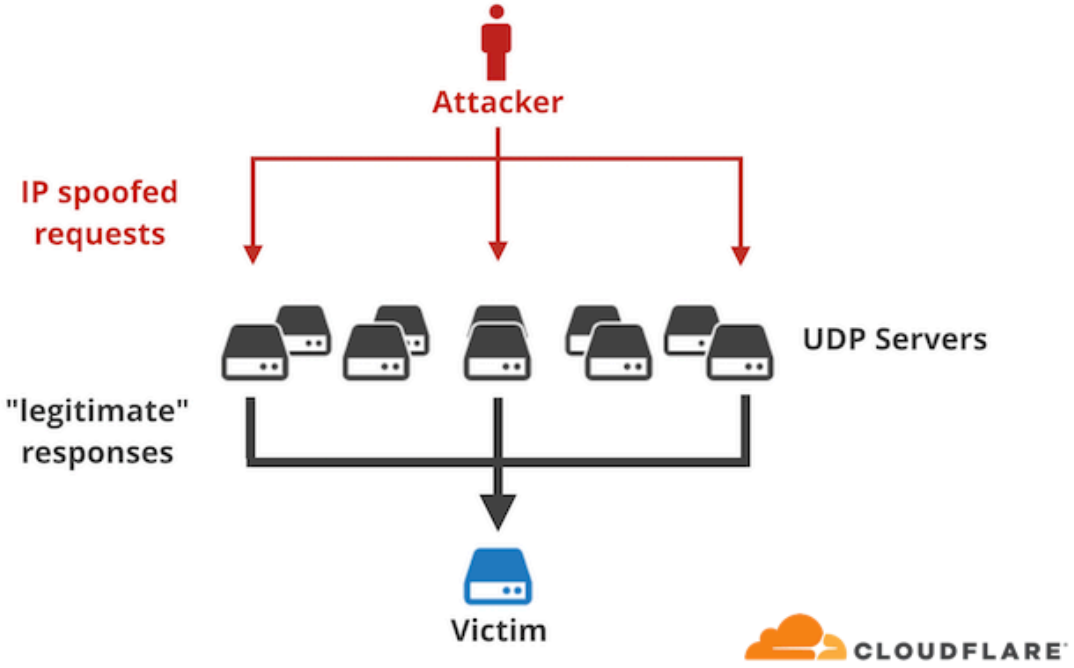
4 min read


Over last couple of days we've seen a big increase in an obscure amplification attack vector - using the memcached protocol, coming from UDP port 11211.


CC BY-SA 2.0 image by David TrawinIn the past, we have talked a lot about amplification attacks happening on the internet. Our most recent two blog posts on this subject were:

- SSDP amplifications crossing 100Gbps. Funnily enough, since then we were a target of an 196Gbps SSDP attack.
- General statistics about various amplification attacks we see.

The general idea behind all amplification attacks is the same. An IP-spoofing capable attacker sends forged requests to a vulnerable UDP server. The UDP server, not knowing the request is forged, politely prepares the response. The problem happens when thousands of responses are delivered to an unsuspecting target host, overwhelming its resources - most typically the network itself.



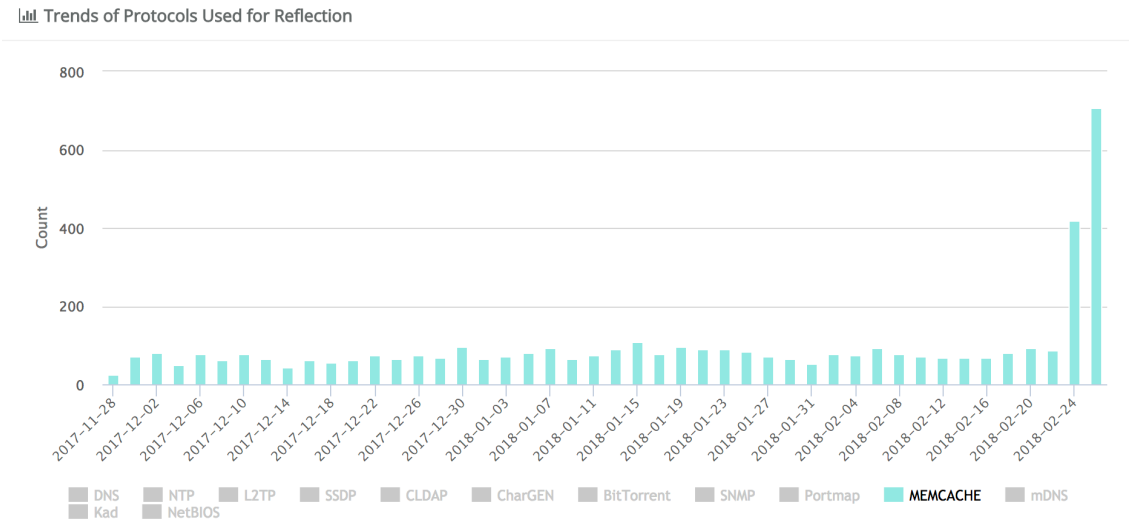

Amplification attacks are effective, because often the response packets are much larger than the request packets. A carefully prepared technique allows an attacker with limited IP spoofing capacity (such as 1Gbps) to launch very large attacks (reaching 100s Gbps) "amplifying" the attacker's bandwidth.

## Memcrashed

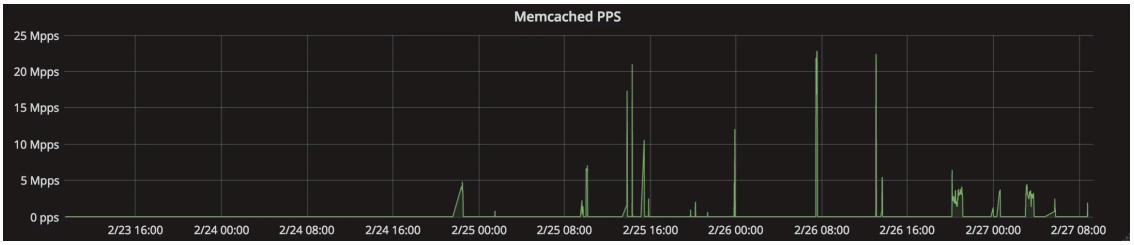
Obscure amplification attacks happen all the time. We often see "chargen" or "call of duty" packets hitting our servers.

A discovery of a new amplification vector though, allowing very great amplification, happens rarely. This new memcached UDP DDoS is definitely in this category.

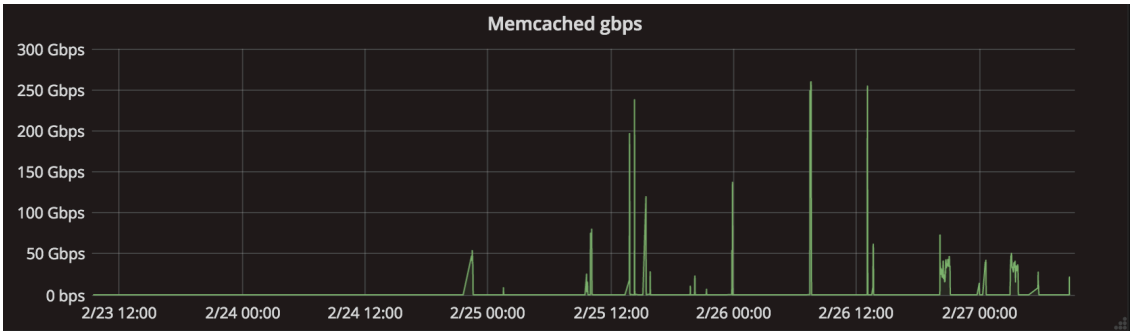
The DDosMon from Qihoo 360 monitors amplification attack vectors and this chart shows recent memcached/11211 attacks:




The number of memcached attacks was relatively flat, until it started spiking just a couple days ago. Our charts also confirm this, here are attacks in packets per second over the last four days:




While the packets per second count is not that impressive, the bandwidth generated is:




At peak we've seen 260Gbps of inbound UDP memcached traffic. This is massive for a new amplification vector. But the numbers don't lie. It's possible because all the reflected packets are very large. This is how it looks in tcpdump:

```
 $ tcpdump -n -t -r memcrashed.pcap udp and port 11211 -c 10
IP 87.98.205.10.11211 > 104.28.1.1.1635: UDP, length 13
IP 87.98.244.20.11211 > 104.28.1.1.41281: UDP, length 1400
IP 87.98.244.20.11211 > 104.28.1.1.41281: UDP, length 1400
IP 188.138.125.254.11211 > 104.28.1.1.41281: UDP, length 1400
IP 188.138.125.254.11211 > 104.28.1.1.41281: UDP, length 1400
IP 188.138.125.254.11211 > 104.28.1.1.41281: UDP, length 1400
```

```
IP 188.138.125.254.11211 > 104.28.1.1.41281: UDP, length 1400
IP 188.138.125.254.11211 > 104.28.1.1.41281: UDP, length 1400
IP 5.196.85.159.11211 > 104.28.1.1.1635: UDP, length 1400
IP 46.31.44.199.11211 > 104.28.1.1.6358: UDP, length 13
```

The majority of packets are 1400 bytes in size. Doing the math 23Mpps x 1400 bytes gives 257Gbps of bandwidth, exactly what the chart shows.

### Memcached does UDP?

I was surprised to learn that memcached does UDP, but there you go! The protocol specification shows that it's one of *the best protocols to use for amplification ever*! There are absolutely zero checks, and the data *WILL* be delivered to the client, with blazing speed! Furthermore, the request can be tiny and the response huge (up to 1MB).

Launching such an attack is easy. First the attacker implants a large payload on an exposed memcached server. Then, the attacker spoofs the "get" request message with target Source IP.

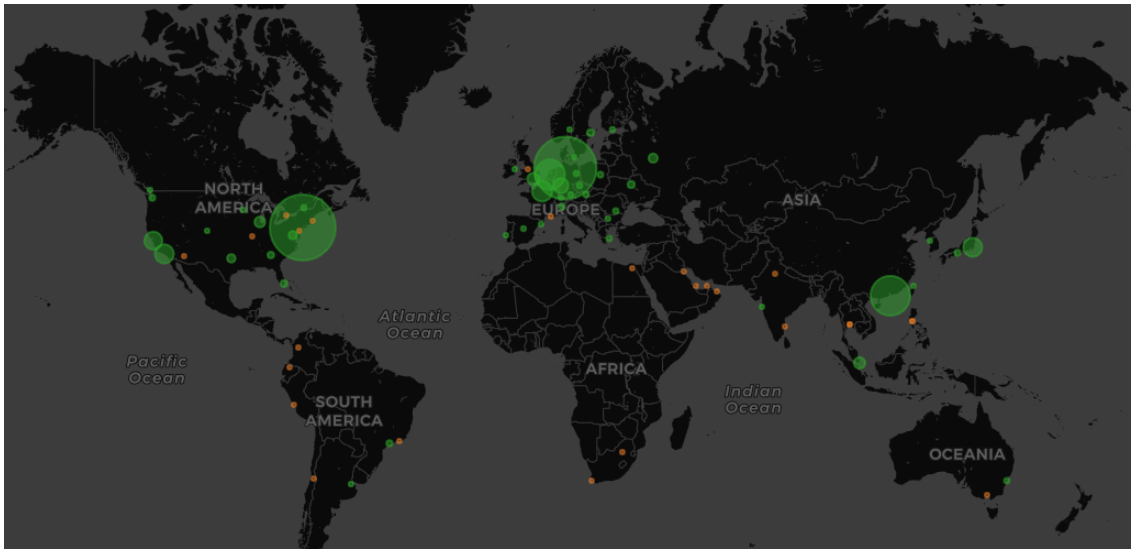
Synthetic run with Tcpdump shows the traffic:

```
 $ sudo tcpdump -ni eth0 port 11211 -t
IP 172.16.170.135.39396 > 192.168.2.1.11211: UDP, length 15
IP 192.168.2.1.11211 > 172.16.170.135.39396: UDP, length 1400
IP 192.168.2.1.11211 > 172.16.170.135.39396: UDP, length 1400
...(repeated hundreds times)...
```

15 bytes of request triggered 134KB of response. This is amplification factor of 10,000x! In practice we've seen a 15 byte request result in a 750kB response (that's a 51,200x amplification).

### Source IPs

The vulnerable memcached servers are all around the globe, with higher concentration in North America and Europe. Here is a map of the source IPs we've seen in each of our 120+ points of presence:

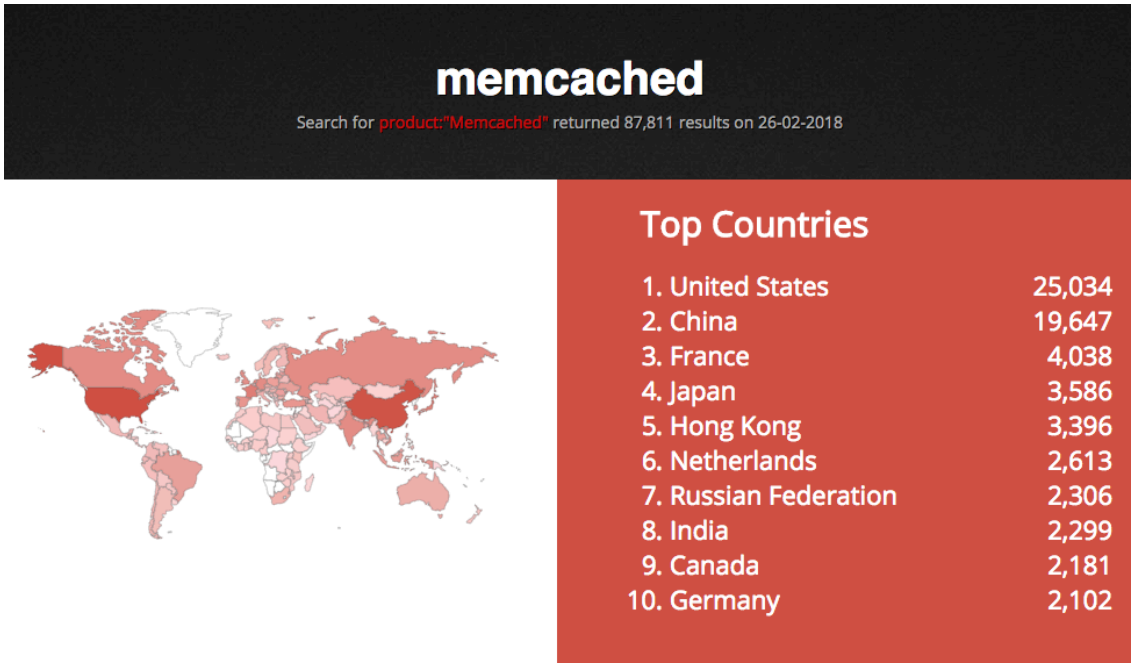



Interestingly our datacenters in EWR, HAM and HKG see disproportionally large numbers of attacking IPs. This is because most of the vulnerable servers are located in major hosting providers. The AS numbers of the IPs that we've seen:

| ips | srcASN | ASName |
|---|---|---|
| 578 | AS16276 | OVH |
| 468 | AS14061 | DIGITALOCEAN-ASN - DigitalOcean, LLC |
| 231 | AS7684 | SAKURA-A SAKURA Internet Inc. |
| 199 | AS9370 | SAKURA-B SAKURA Internet Inc. |
| 165 | AS12876 | AS12876 |
| 119 | AS9371 | SAKURA-C SAKURA Internet Inc. |
| 104 | AS16509 | AMAZON-02 - Amazon.com, Inc. |
| 102 | AS24940 | HETZNER-AS |
| 81 | AS26496 | AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC |
| 74 | AS36351 | SOFTLAYER - SoftLayer Technologies Inc. |
| 65 | AS20473 | AS-CHOOPA - Choopa, LLC |
| 49 | AS49981 | WORLDSTREAM |
| 48 | AS51167 | CONTABO |
| 48 | AS33070 | RMH-14 - Rackspace Hosting |
| 45 | AS19994 | RACKSPACE - Rackspace Hosting |
| 44 | AS60781 | LEASEWEB-NL-AMS-01 Netherlands |
| 42 | AS45899 | VNPT-AS-VN VNPT Corp |
| 41 | AS2510 | INFOWEB FUJITSU LIMITED |
| 40 | AS7506 | INTERQ GMO Internet,Inc |
| 35 | AS62567 | DIGITALOCEAN-ASN-NY2 - DigitalOcean, LLC |
| 31 | AS8100 | ASN-QUADRANET-GLOBAL - QuadraNet, Inc |
| 30 | AS14618 | AMAZON-AES - Amazon.com, Inc. |
| 30 | AS31034 | ARUBA-ASN |

Most of the memcached servers we've seen were coming from AS16276 - OVH, AS14061 - Digital Ocean and AS7684 - Sakura.

In total we've seen only 5,729 unique source IPs of memcached servers. We're expecting to see much larger attacks in future, as Shodan reports 88,000 open memcached servers:




## Let's fix it up

It's necessary to fix this and prevent further attacks. Here is a list of things that should be done.

### Memcached Users

If you are using memcached, please disable UDP support if you are not using it. On memcached startup you can specify `--listen 127.0.0.1` to listen only to localhost and `-U 0` to disable UDP completely. *By default memcached listens on INADDR_ANY and runs with UDP support ENABLED*. Documentation:

- https://github.com/memcached/memcached/wiki/ConfiguringServer#udp

You can easily test if your server is vulnerable by running:

```
 $ echo -en "\x00\x00\x00\x00\x01\x00\x00stats\r\n" | nc -q1 -u 127.0.0.1 11211
STAT pid 21357
STAT uptime 41557034
STAT time 1519734962
...
```

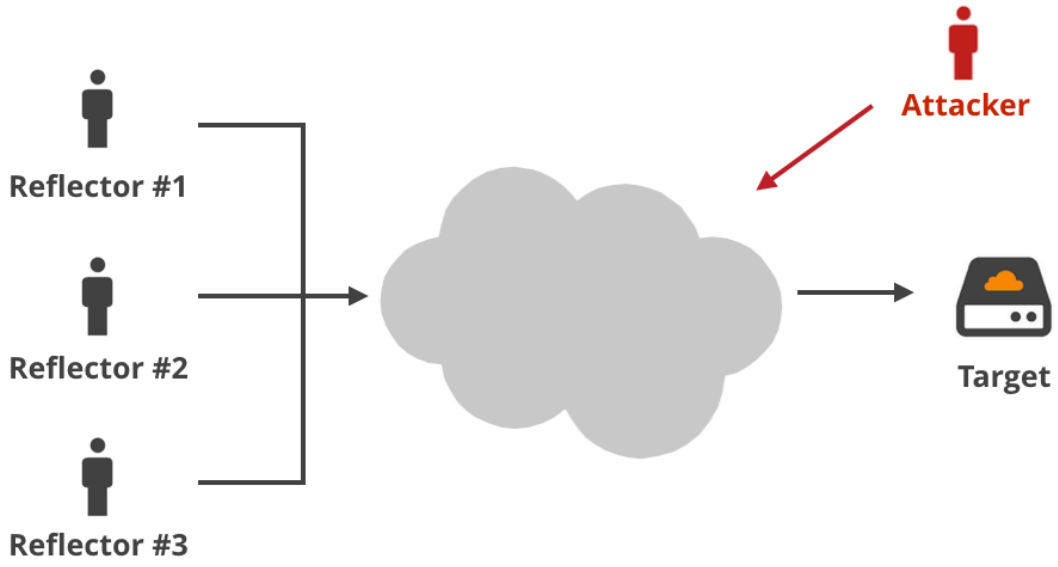
If you see non-empty response (like the one above), your server is vulnerable.

### System administrators

Please ensure that your memcached servers are firewalled from the internet! To test whether they can be accessed using UDP I recommend the `nc` example above, to verify if TCP is closed run `nmap`:

```
 $ nmap TARGET -p 11211 -sU -sS --script memcached-info
Starting Nmap 7.30 ( https://nmap.org ) at 2018-02-27 12:44 UTC
Nmap scan report for xxxx
Host is up (0.011s latency).
PORT      STATE         SERVICE
11211/tcp open          memcache
| memcached-info:
|   Process ID           21357
|   Uptime               41557524 seconds
|   Server time          2018-02-27T12:44:12
|   Architecture         64 bit
|   Used CPU (user)      36235.480390
|   Used CPU (system)    285883.194512
|   Current connections  11
|   Total connections    107986559
|   Maximum connections  1024
|   TCP Port             11211
|   UDP Port             11211
|_  Authentication       no
11211/udp open|filtered memcache
```

**Internet Service Providers**




In order to defeat such attacks in future, we need to fix vulnerable protocols and also IP spoofing. As long as IP spoofing is permissible on the internet, we'll be in trouble.

Help us out by tracking who is behind these attacks. We must know not who has problematic memcached servers, but *who sent them queries in the first place*. We can't do this without your help!

**Developers**

Please please please: Stop using UDP. If you must, please don't enable it by default. If you do not know what an amplification attack is I hereby forbid you from ever typing `SOCK_DGRAM` into your editor.

We've been down this road so many times. DNS, NTP, Chargen, SSDP and now memcached. If you use UDP, you must always respond with strictly a *smaller* packet size then the request. Otherwise your protocol will be abused. Also remember that people do forget to set up a firewall. Be a nice citizen. Don't invent a UDP-based protocol that lacks authentication of any kind.

## That's all

It's anyone's guess how large the memcached attacks will become before we clean the vulnerable servers up. There were already rumors of 0.5Tbps amplifications in the last few days, and this is just a start.

Finally, you are OK if you are a Cloudflare customer. Cloudflare's Anycast architecture works well to distribute the load in case of large amplification attacks, and unless your origin IP is exposed, you are safe behind Cloudflare.

## Prologue

A comment (below) points out that the possibility of using memcached for DDoS was discussed in a 2017 presentation.

**Update**We received a word from Digital Ocean, OVH, Linode and Amazon that they tackled the memcached problem, their networks should not be a vector in future attacks. Hurray!

---



DDoSDevelopersMitigationReliabilityAttacksVulnerabilities

---