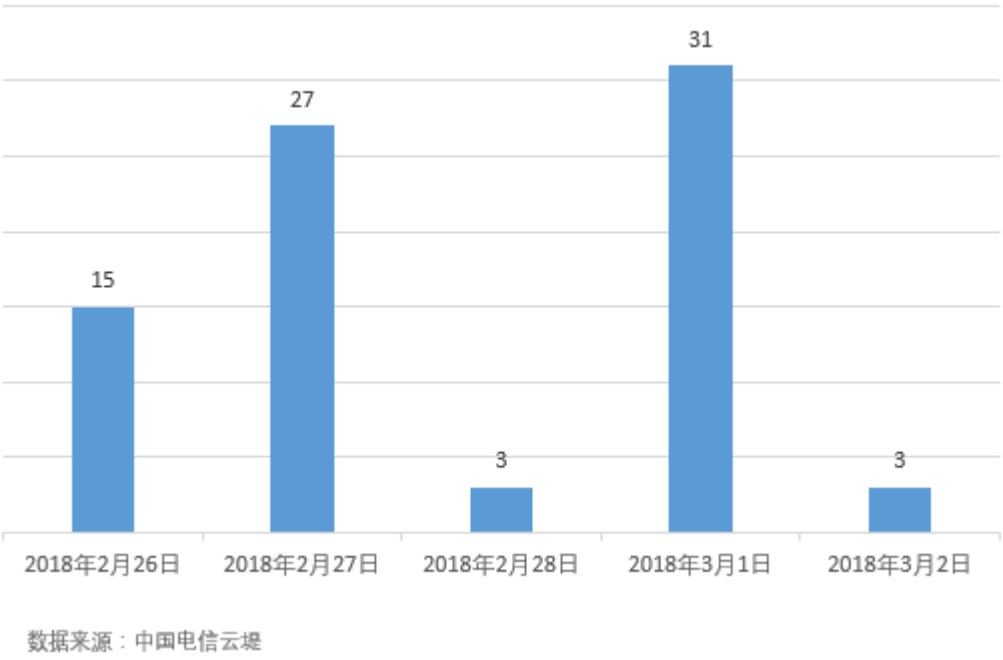
深度剖析 Memcached 超大型 DRDoS 攻击

——绿盟科技&电信云堤联合发布

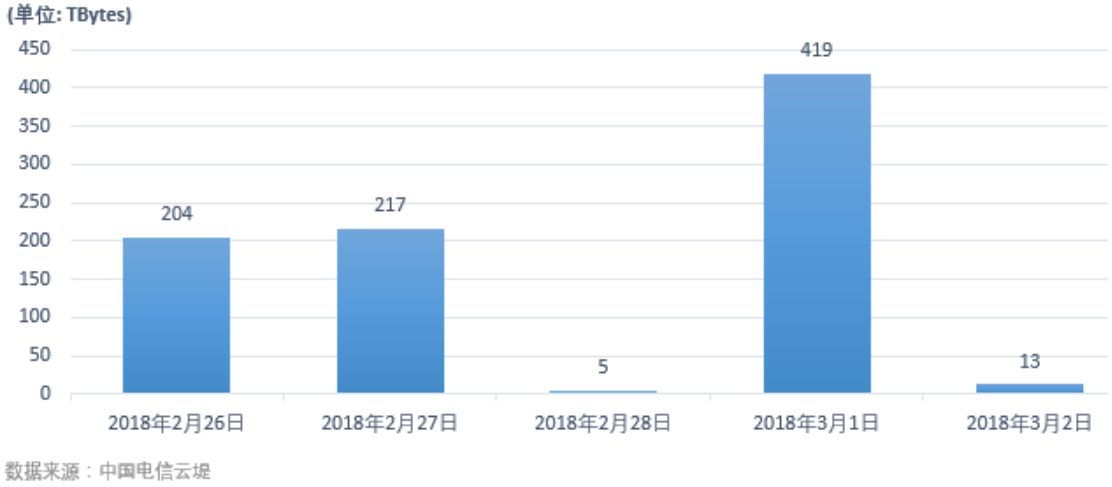
近日，国内外多家安全公司和机构发布了 Memcached 超级 DRDoS（Distributed Reflection Denial of Service）攻击的预警，引发各方关注。据我们的监控显示，目前该攻击的最大峰值流量已经达到了 1.35T。而在 2 月 27 号，Memcached 的反射攻击事件流量范围不过几百兆到最大 500G 左右。几日之隔，攻击峰值的历史纪录就迅速被翻倍刷新，并且攻击发生的频率从一天十几次到几百次，呈现爆发式增长。这是要搞大事情！

1、事件回顾

根据中国电信云堤的攻击监控数据显示，从本周一至周五（2 月 26 日至 3 月 2 日 06:00）短短 5 天内，全球就发生了 79 起利用 Memcached 协议的反射放大攻击。日攻击总流量最高达到 419TBytes。

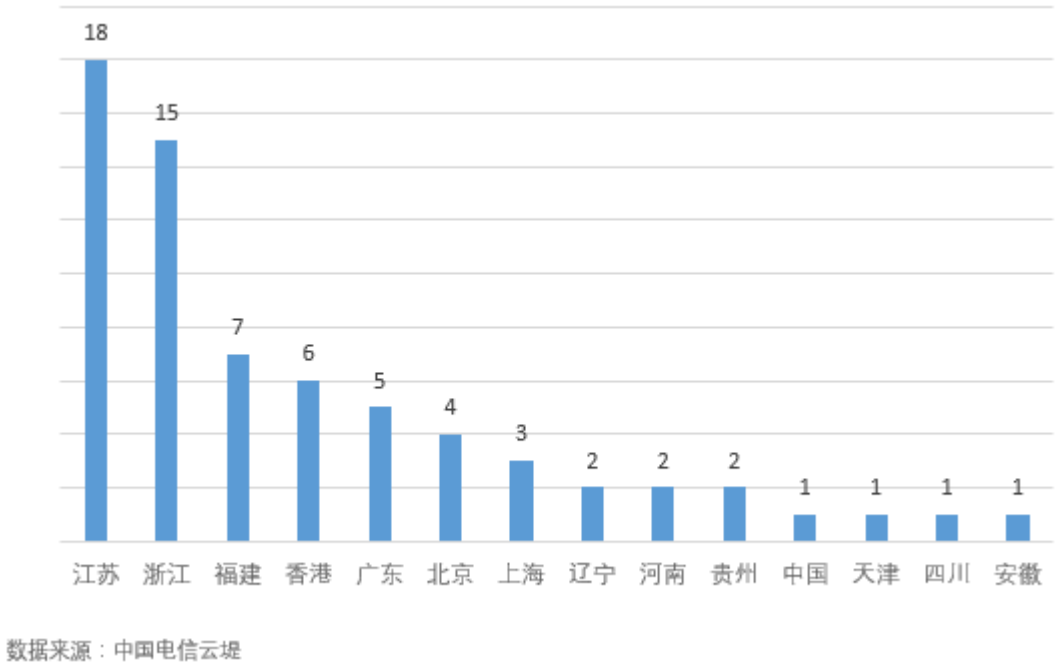


Memcached 反射放大攻击日攻击次数



Memcached 反射放大攻击日攻击总流量

其中，针对我国境内的 Memcached 反射放大攻击就有 68 次，江苏、浙江两省被攻击频繁。针对我国境内的攻击，单次攻击最高攻击峰值达 505Gbps。攻击持续时间最长的一次发生在 3 月 1 日，持续 1.2 小时，总攻击流量达 103.8TBytes。



中国各省份地区 Memcached 反射放大攻击次数

从影响范围来看，所有互联网的业务都可能成为 Memcached DRDoS 的攻击对象。一方面带宽或业务遭受超大流量的攻击，导致出口带宽完全被占满，正

常业务无法访问；另一方面企业内部的 Memcached 系统可能被不法分子利用成为攻击帮凶。我们呼吁各地区、各行业客户保持高度警惕，谨防 Memcached 反射攻击对服务器造成直接冲击或利用 Memcached 反射攻击作为障眼法混合其他攻击造成信息安全危害。

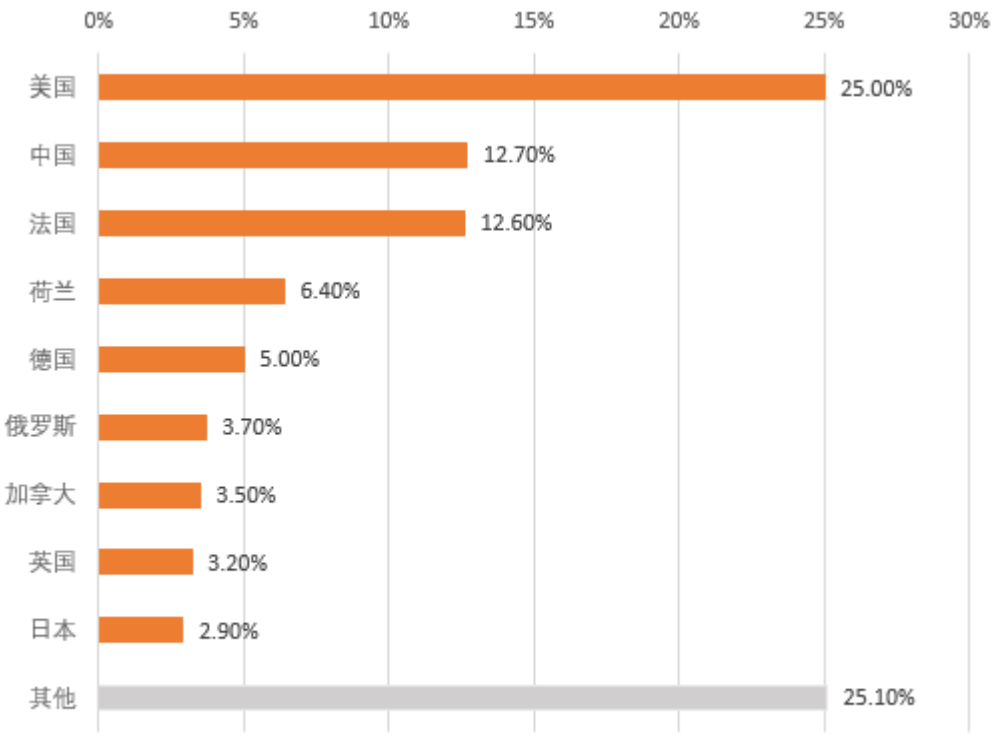
2、攻击分析

2.1 什么是 Memcached？

Memcached 是一个高性能的开源分布式内存对象缓存系统，主要用于提高 Web 应用的扩展性，能够有效解决大数据缓存的很多问题，在全球范围内都有广泛使用。Memcached 基于内存的 key-value 存储小块数据，并使用该数据完成数据库调用、API 调用或页面渲染等。攻击者正是利用 key-value 这项功能构造了大流量的 Memcached 反射攻击。这一点在后文会详细介绍。

2.2 Memcached 分布情况

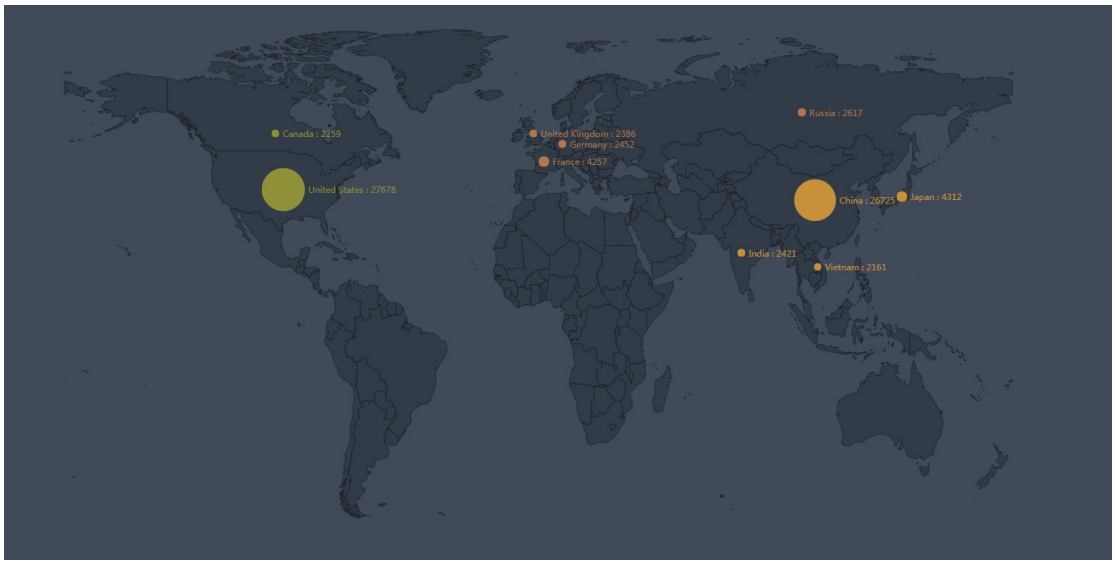
最新统计显示，全球总共有 3790 个 Memcached 服务器被利用参与到这些 Memcached 反射放大攻击。这些被利用反射源遍布于全球 96 个国家或地区范围内。其中，美国就占了全球的 1/4。



数据来源：中国电信云堤

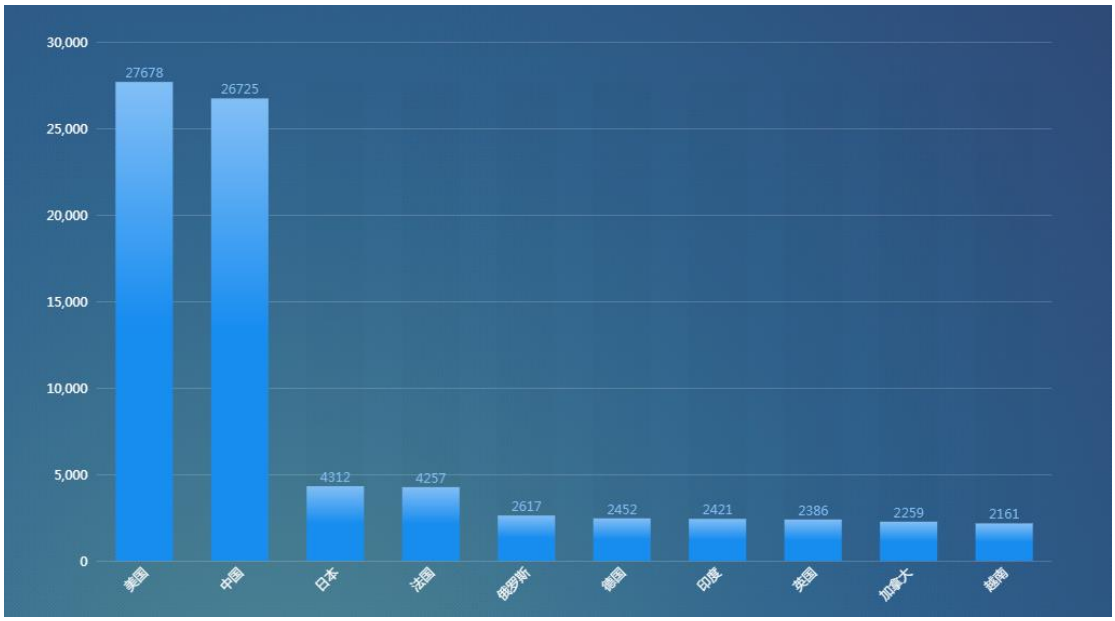
分布在中国地区的被利用的 Memcached 服务器位列第二位，占比 12.7%。在中国各省份占比如下所示，广东、北京、浙江为 TOP3。

绿盟科技威胁情报中心（NSFOCUS Network Threat Intelligence，简称 NTI）的统计结果显示，全球范围内存在被利用风险的 Memcached 服务器为 104,506 台。分布情况如下：



数据来源：绿盟威胁情报中心

从地理分布来看，美国可被利用的 Memcached 服务器最多，其次是中国。



数据来源：绿盟威胁情报中心

这些活跃的 Memcached 反射器为构造超级 DRDoS 攻击提供了有力的先决条件。如果不及时修复治理，预计基于 Memcached 反射攻击的攻击事件会继续增加，后果不敢想象。

2.3 Memcached 如何形成 DRDoS 攻击？

Memcached 反射攻击的构造过程分为如下 3 步；

1. 收集反射器 IP

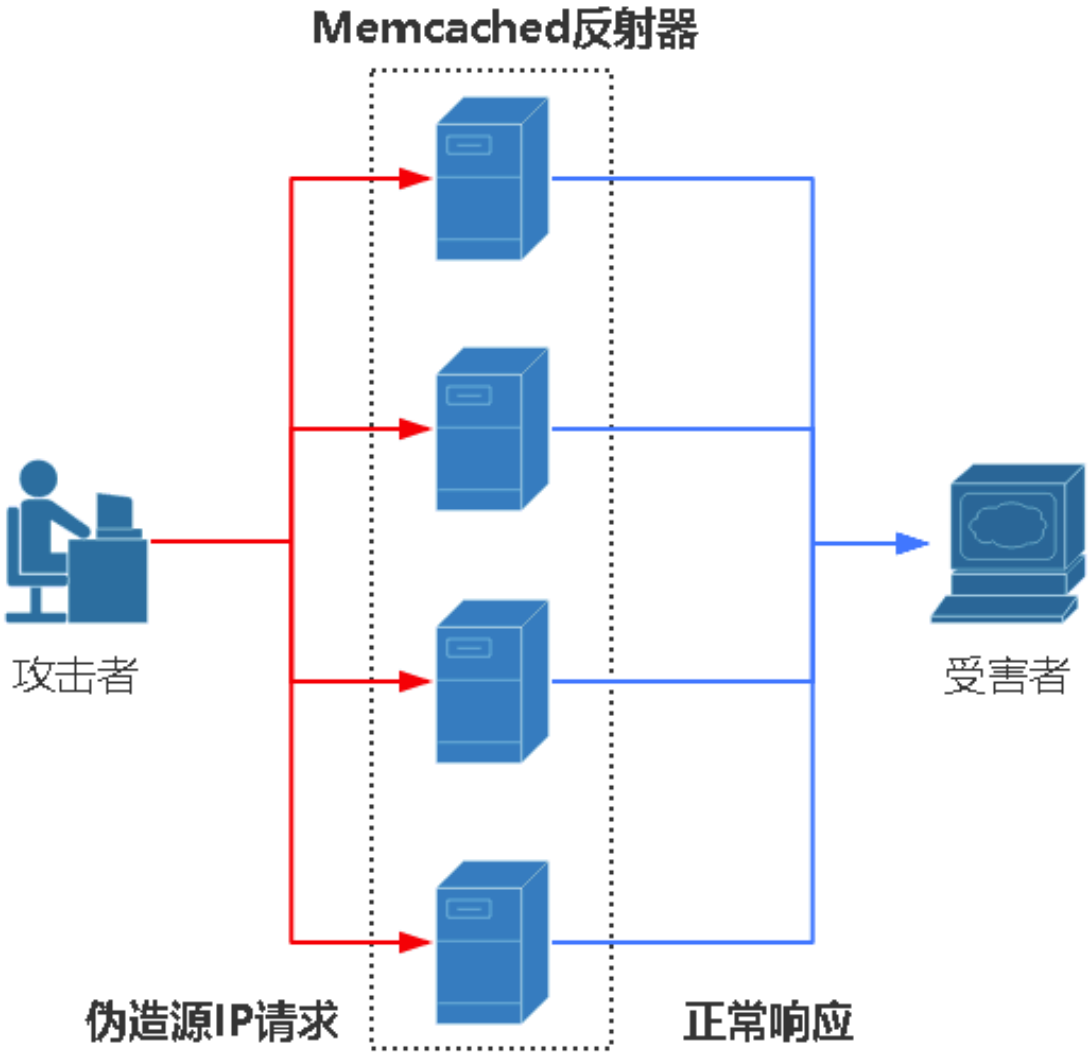
通过 NTI/Shodan 等情报引擎找到开放的 Memcached 系统，获取系统 IP；

2. 配置反射器

利用开放的 Memcached 系统作为反射器，并修改 key-value 配置实现较大的存储容量，为构造反射放大攻击进行准备；

3. 发起反射攻击

攻击者将自身 IP 伪造成攻击的目标地址，并向 Memcached 反射器发送请求读取 Memcached 在 key-value 中存储的信息。Memcached 在收到请求后向伪造的虚假源 IP 进行回复，从而形成反射。



Memcached 反射攻击示意图

当大量 Memcached 被同时利用，并用同一个伪造源 IP 进行回复，就轻而易举地形成了针对这个伪造源（受害者）的大流量 DRDoS 攻击。

2.4 Memcached 的攻击特征

DRDoS（Distributed Reflective Denial-of-Service）是 DDoS 攻击分类中的一种。绿盟科技在 2015 年、2016 年及 2017 年发布的 DDoS 态势报告中均有说明（报告下载链接 http://www.nsfocus.com.cn/research/report_3.html）。报告中通过实际案

例及数据统计明确指出了反射攻击的流行性及危害程度，此次 Memcached 反射攻击的爆发进一步表明 DRDoS 攻击的热度还将持续下去。

此前各类安全厂商监测到的 DRDoS 攻击主要是 SSDP 反射、DNS 反射、NTP 反射等。下表（引自 US-Cert）详细列举了各类反射攻击的放大倍数。

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP	56 to 70	——
TFTP	60	——
Memcache	**10,000 to 51,000**	**——**

仅从放大倍数来看，Memcached 反射攻击的危害程度远远高于其他反射攻击类型，US-Cert 提供的数据显示它能够实现 51,000 倍的放大效果。

与其他反射攻击相比，Memcached 如何实现这么多倍的放大效果呢？其中的重要原因就是 Memcached 的 key-value 功能。前文提到 key-value 的作用是决定存储容量的大小，正常情况下 key-value 的值通常不超过几千字节。当 Memcached 被攻击者利用作为反射器时，key-value 的值经过修改可以达到 100 万字节以上。

攻击过程我们通过实验室也进行了完整复现。

第一步，通过命令修改 Memcached 上的 key-value 参数，以提升放大倍数。

send = "set t 0 900 1048501" + "\r\n" + 'a' * 1048501 + "\r\n"

socket.sendall(send)

经验证，key-value 的最大值为 1048501。

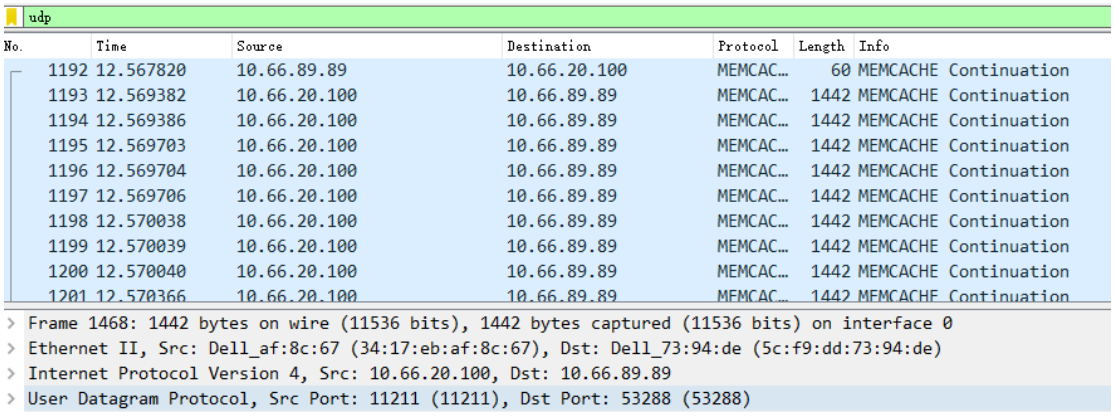
```
set test 0 900 1048502
SERVER_ERROR object too large for cache
```

第二步通过 get 命令读取 Memcached 的存储信息，并反射到目标 IP。

get="\x00\x00\x00\x00\x00\x01\x00\x00get t\r\n"

socket.sendto(get, (host, 11211))

形成的攻击报文如下：

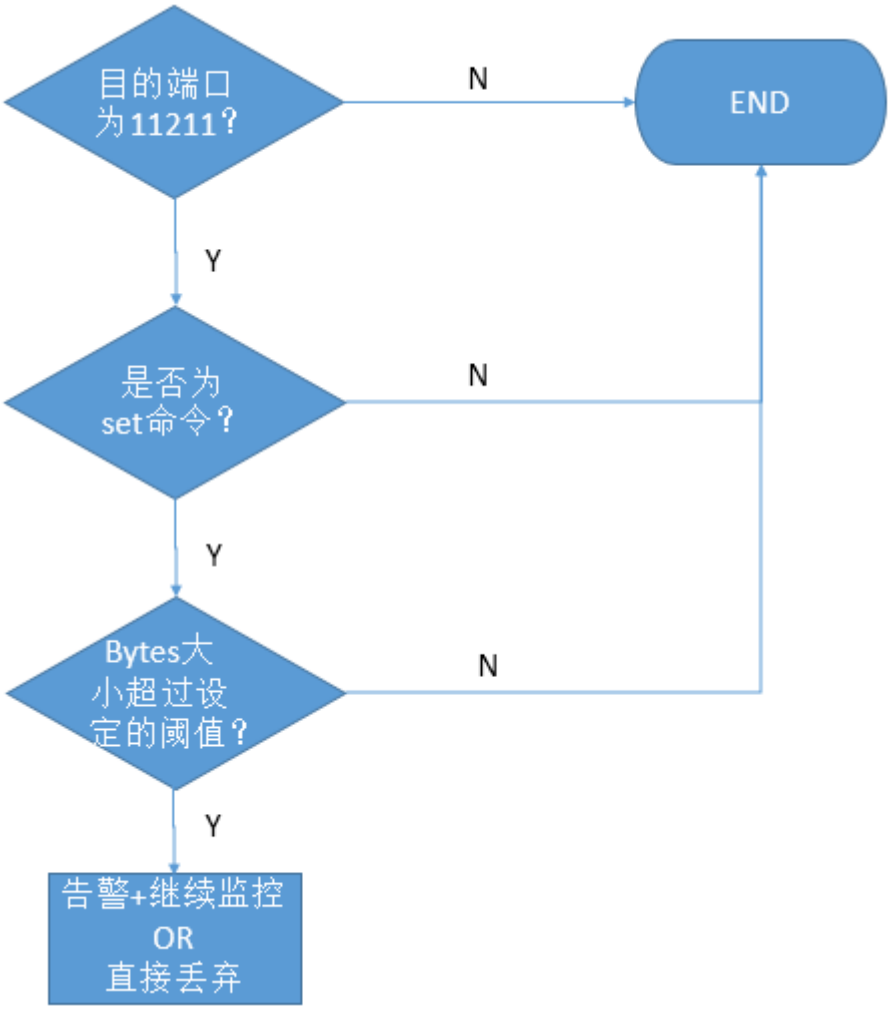


触发 Memcached 反射攻击的请求报文最小为 15 字节，包含为 8 字节（RFC 规定字段）+3 字节 (get)+1（空格）+最小为 1 字节（键的名称 ）+2 字节 (\r\n)，而返回的请求数据达到 105 万字节，理论上可放大到接近 7 万倍。如此强悍的放大攻击，与其他各类 DRDoS 攻击形成断崖式的差距对比。

3、Memcached 攻击防护加固建议

3.1 Memcached 系统自查建议

攻击的形成过程为我们提供了一个很好的预警思路，安全产品可针对 Memcached 的 key-value 配置进行检测，在 Memcached 系统被利用成为攻击源之前就进行拦截。检测流程如下：



（1）检测目的端口为 11211 的 TCP 或 UDP 报文（确保是 Memcached 服务器）；

（2）检测报文是否为 set 命令（set 命令格式参见附录），如果是则执行（3），否则结束检测；

（3）检测 set 命令后面的 bytes 字段值（如下图中标注的 1048501），是否超过设定的阈值，如果是，则可以怀疑该报文存在异常；

```
▸ Frame 4: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: Dell_73:94:de (5c:f9:dd:73:94:de), Dst: Dell_af:8c:67 (34:17:eb:af:8c:67)
▸ Internet Protocol Version 4, Src: 10.66.89.89, Dst: 10.66.20.100
▸ Transmission Control Protocol, Src Port: 53783 (53783), Dst Port: 11211 (11211), Seq: 1, Ack: 1, Len: 1460

0000  34 17 eb af 8c 67 5c f9  dd 73 94 de 08 00 45 00   4....g\. .s....E.
0010  05 dc 5c 13 40 00 40 06  00 00 0a 42 59 59 0a 42   ..\.@.@. ...BYY.B
0020  14 64 d2 17 2b cb ef 20  43 1f 9d b6 ab 9e 50 10   .d..+..  C.....P.
0030  40 29 88 0f 00 00 73 65  74 20 74 65 73 74 20 30   @)....se t test 0
0040  20 39 30 30 20 31 30 34  38 35 30 31 0d 0a 61 61    900 104 8501..aa
0050  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0060  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0070  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0080  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0090  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00a0  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00b0  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00c0  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
00d0  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
```

（4）检测到该类异常控制报文后，可有如下两种处理方式：

a．告警并监控。为了防止被误杀，建议同时监控该 Memcached 服务器后面的流量变化来进一步判断该服务器是否被用做了反射器。

b. 直接丢弃。如果有足够的证据表明该记录是恶意添加的，直接丢弃可以保证服务器不被当做反射器。

自查举例：假设下图是公网的一台 Memcached 服务器上获取的数据。

```
stats sizes
STAT 96 1
STAT 864 1
STAT 896 89
STAT 928 52
STAT 960 24
STAT 992 9
STAT 1024 10
STAT 1088 2
STAT 1120 1
STAT 1184 1
STAT 50080 1
STAT 55072 1
STAT 65088 2
STAT 1000064 1
END
```

通常情况下，多数 value 的大小都在 64K 以内，而最后一条的达到了将近 1M，与其他记录有很明显的差别，基本上可以判断该记录存在问题，该服务器可能已经被利用。

3.2 Memcached 攻击流量清洗

面对如此大规模、大范围的 DDoS 攻击威胁，所有网络安全节点都应该加强防范，从攻击防护和外发清洗两方面入手，充分保障基础设施和业务流量的安全。针对此攻击，我们提供如下防护建议：

- 运营商。

运营商及 IDC 处于网络上游，拥有强大的带宽资源，是攻击最直接的受害者，也是防护的第一道屏障。运营商能够灵活控制路由策略和防护策略进行快速过滤。

1）在边界配置 UDP 访问控制规则，将源端口为 11211 的报文进行阻断或限速；

2）在边界配置 BGP FlowSpec 策略，对源端口为 11211 的 UDP 流量进行阻断或限速；

3）利用 DDoS 防护设备将源端口为 11211 的 UDP 流量进行阻断或限速。

- 企业用户

企业用户通常贴近服务终端，熟悉掌握自身业务流量特点，策略配置更加明确，灵活性强。

1）大型企业客户可以采用和运营商相同的策略，在出口边界设备配置 UDP 访问控制规则或 BGP FlowSpec 策略对源端口为 11211 的 UDP 流量进行阻断或限速；

2）不具备出口路由配置权限的企业客户，可以在抗 DDoS 等设备上配置防护策略，对源端口为 11211 的 UDP 流量进行阻断或限速；

3）考虑企业出口带宽可能被打满的情况，企业客户可通过运营商或云清洗服务在上游执行清洗策略，策略内容同样是对源端口为 11211 的 UDP 流量进行阻断或限速。

3.3 Memcached 系统防护加固

对于正在使用 Memcached 系统的用户，为了避免被攻击者利用，使 Memcached 成为攻击源，对外发起攻击流量，影响自身系统性能，我们提供如下几点建议。

1）在边界网络设备上配置 URPF 策略，过滤外发的虚假源 IP 报文；

2）在 Memcached 系统前进行深度检测，直接过滤报文特征中 set key 0 900 64000 的第三个字段过大的数据包，这样做可以在 Memcached 系统被修改利用成为攻击源前进行拦截；

3）对 Memcached 服务进行安全检查，查看 Memcached 服务是否监听 UDP 端口。查找 Memcached 进程，查看是否有-l 参数，如果没有则默认为 0.0.0.0。若 Memcached 服务不需要监听 UDP，禁用 UDP。详情参考 Memcached 官方文档：https://github.com/memcached/memcached/wiki/ConfiguringServer#udp

附录

set 命令的基本语法格式如下：

```
set key flags exptime bytes [noreply]

value
```

参数说明如下：

key：键值 key-value 结构中的 key，用于查找缓存值。

flags：包括键值对的整型参数，客户机使用它存储关于键值对的额外信息 。

exptime：在缓存中保存键值对的时间长度（以秒为单位，0 表示永远）

bytes：在缓存中存储的字节数

noreply（可选）： 该参数告知服务器不需要返回数据

value：存储的值（始终位于第二行）（可直接理解为 key-value 结构中的 value）