DDoS 反射放大攻击全球探测分析

第五版

知道创宇 404 实验室

V 5.0

2019-05-06

1. 更新情况

版本	时间	描述
第一版	2017/08/07	完成第一轮数据统计，输出报告，完善文档格式
第二版	2017/08/14	完成第二轮数据统计，输出报告，完善文档格式
第三版	2017/11/15	完成第三轮数据统计，在第二轮的基础上增加对 cldap 的探测
第四版	2018/03/05	完成第四轮数据统计，在第三轮的基础上增加对 Memcached 的探测
第五版	2019/05/06	在第四轮数据统计基础上，增加对 CoAP 的探测，并完善为第五版

2. 概述

DDos 攻击是一种耗尽资源的网络攻击方式，攻击者通过大流量攻击，有针对性的漏洞攻击等耗尽目标主机的资源来达到拒绝服务的目的。

反射放大攻击是一种具有巨大攻击力的 DDoS 攻击方式。攻击者只需要付出少量的代价，即可对需要攻击的目标产生巨大的流量，对网络带宽资源（网络层）、连接资源（传输层）和计算机资源（应用层）造成巨大的压力，2016 年 10 月美国 Dyn 公司的 DNS 服务器遭受 DDoS 攻击，导致美国大范围断网。事后的攻击流量分析显示，DNS 反射放大攻击与 SYN 洪水攻击是作为本次造成美国断网的拒绝服务攻击的主力。由于反射放大攻击危害大，成本低，溯源难，被黑色产业从业者所喜爱。

在 2017/08/03 到 2017/08/06 期间 ZoomEye 网络空间探测引擎对全网进行第一轮的探测，统计可被利用进行 DDoS 反射放大攻击的主机数，发布了《DDoS 反射放大攻击全球探测分析-第一版》，之后在 2017/08/11 到 2017/08/13 期间 ZoomEye 网络空间探测引擎再次对全网进行了探测，发布了《DDoS 反射放大攻击全球探测分析-第二版》。之后在 2017/11/13 到 2017/11/15 期间，ZoomEye 网络空间探测引擎探测到了另一个活动频繁的攻击——CLDAP DDoS 反射放大攻击，随后对 DDoS 反射放大攻击进行了第三轮的探测，发布了《DDoS 反射放大攻击全球探测分析-第三版》。

在 2018/03/01，ZoomEye 又探测到在网络空间中频繁活动 Memcached DRDoS， 进行第四轮对 DDoS 反射放大攻击的探测。

在 2019/05/06，ZoomEye 又对网络空间种频繁活动的 CoAP 进行了 DDoS 反射放大攻击探测，并完善为第五版。

3. 第五版放大攻击数据分析

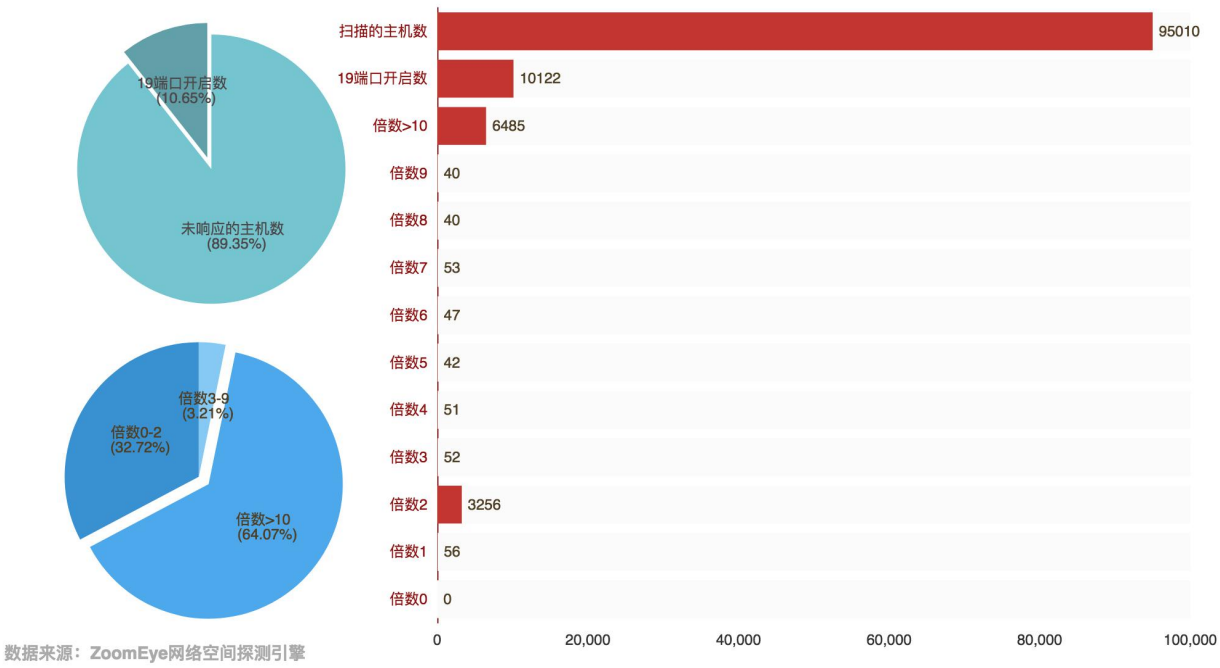
[注：下面数据统计基于第四轮 2018/03/05 与 2019/05/06 CoAP 数据]

2018 年 3 月 5 日，进行了第四轮探测，ZoomEye 网络空间探测引擎在对前面两轮 6 种 DDoS 攻击的探测的基础上，增加了对 Memcached 的探测。2019 年 5 月 6 日，在第四轮基础上，增加了对 CoAP 的探测，并完善为第五版。

3.1. CHARGEN

通过 ZoomEye 网络空间探测引擎获取到 9 万(95,010)台主机开放了 19 端口。然后对这 9 万主机进行放大倍率的探测，实际上只有 1 万(10,122)台主机开启了 19 点端口，占总数的 10.65%。在开启了 19 端口的主机中，有 6 千(6,485)台主机的放大倍数能够达到 10 倍以上，占总数的 64.07%，剩下的主机的放大倍数主要集中在 2 倍。相关数据如图 3.1-1 所示：

3.1-1 Chargen协议19端口探测统计图

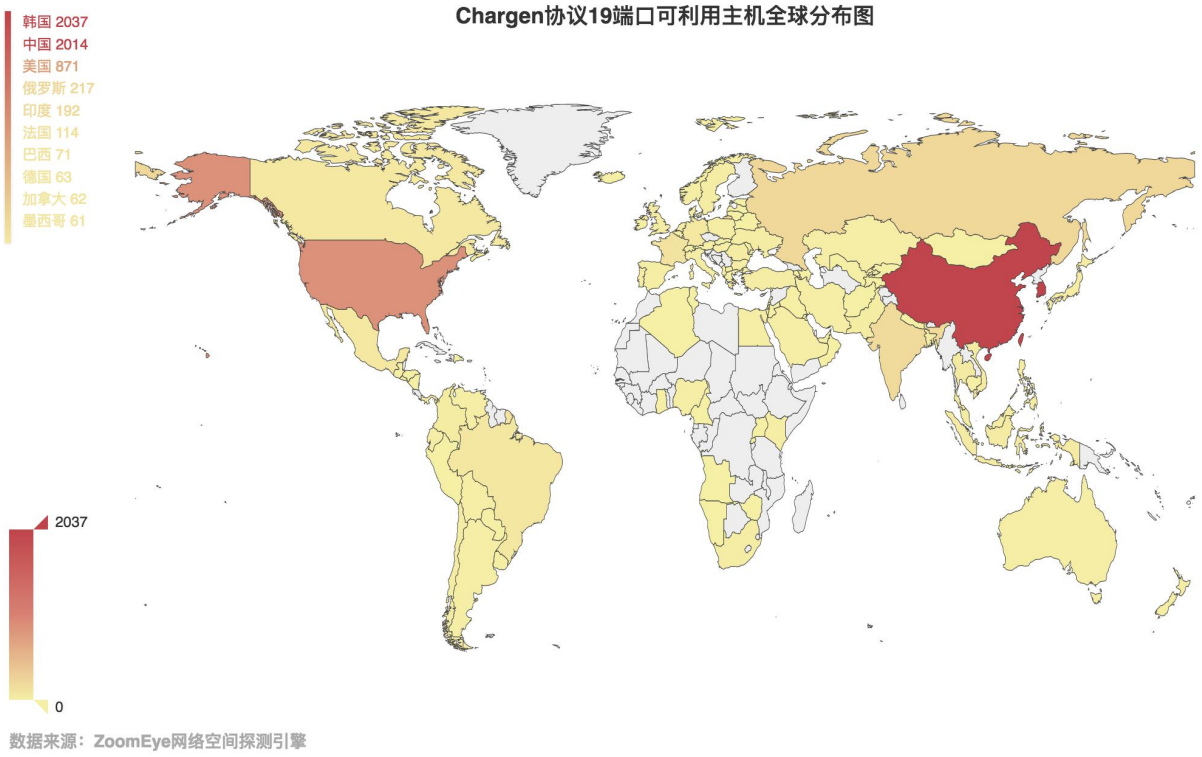


数据来源：ZoomEye网络空间探测引擎

对放大倍数达到 10 以上的主机流量进行统计，我们总共发送了 870KB(891,693 byte)的请求流量，得到了 71M(74,497,401 byte)响应流量，产生了 83 倍的放大流量。假设一台主机 1 分钟内可以成功响应 100 个请求数据包，计算得到攻击流量有 947Mbits/s。本轮探测对最大放大倍数进行了统计，得到了 Chargen 协议单次请求响应最高能放大 319 倍流量。

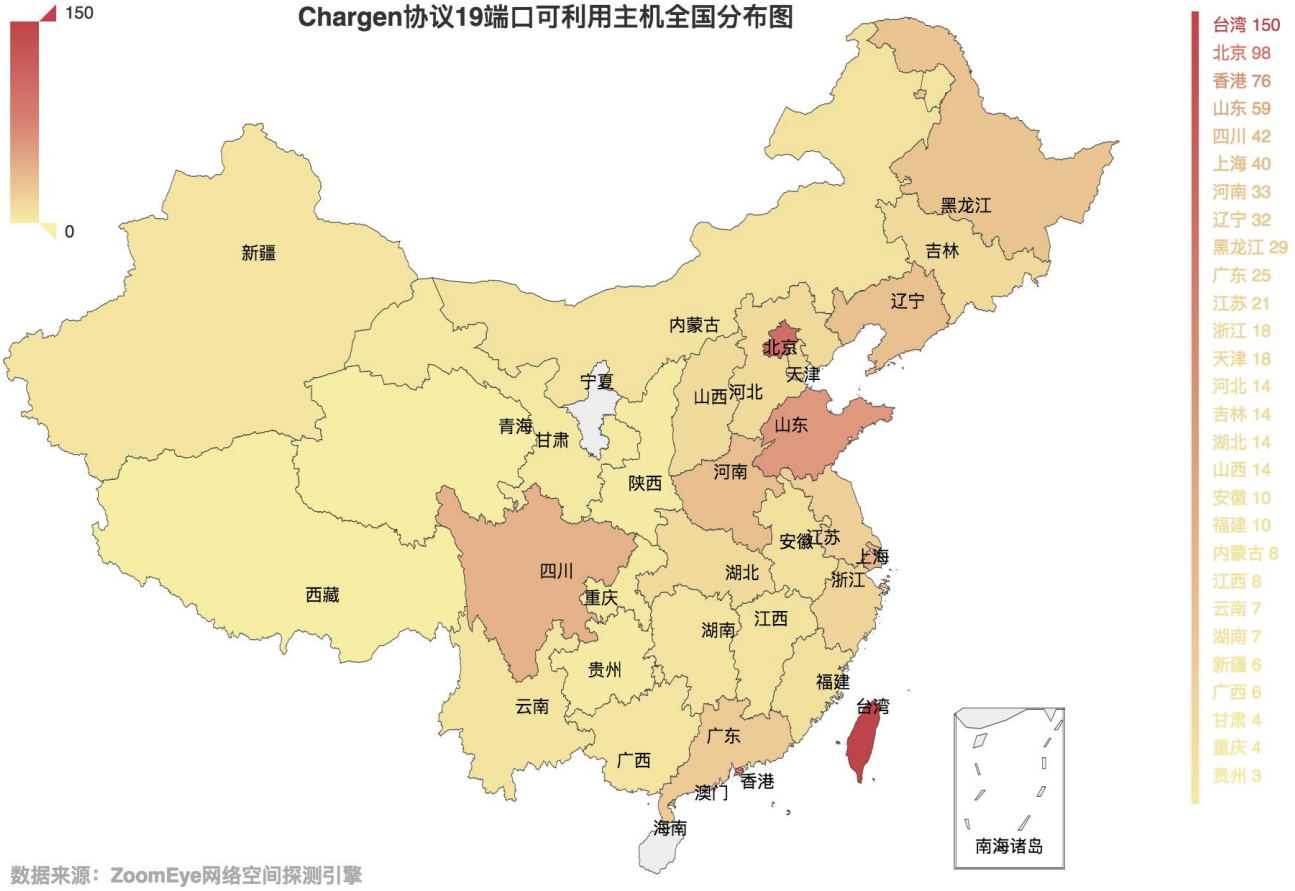
上面的数据和之前两次的的数据进行比较，Chargen DDoS 攻击的危害并没有减小，反而有增大的趋势。

根据 ZoomEye 网络空间探测引擎的探测结果，对可利用的 Chargen 主机进行全球分布统计，见图 3.1-2：



3.1-2 Chargen 协议 19 端口可利用主机全球分布图

从图中可以看出仍然是韩国具有最多数量的可被利用进行 DDos 反射放大攻击的主机，我国排在第二 。下面，对我国各省份的情况进行统计，如图 3.1-3 所示：

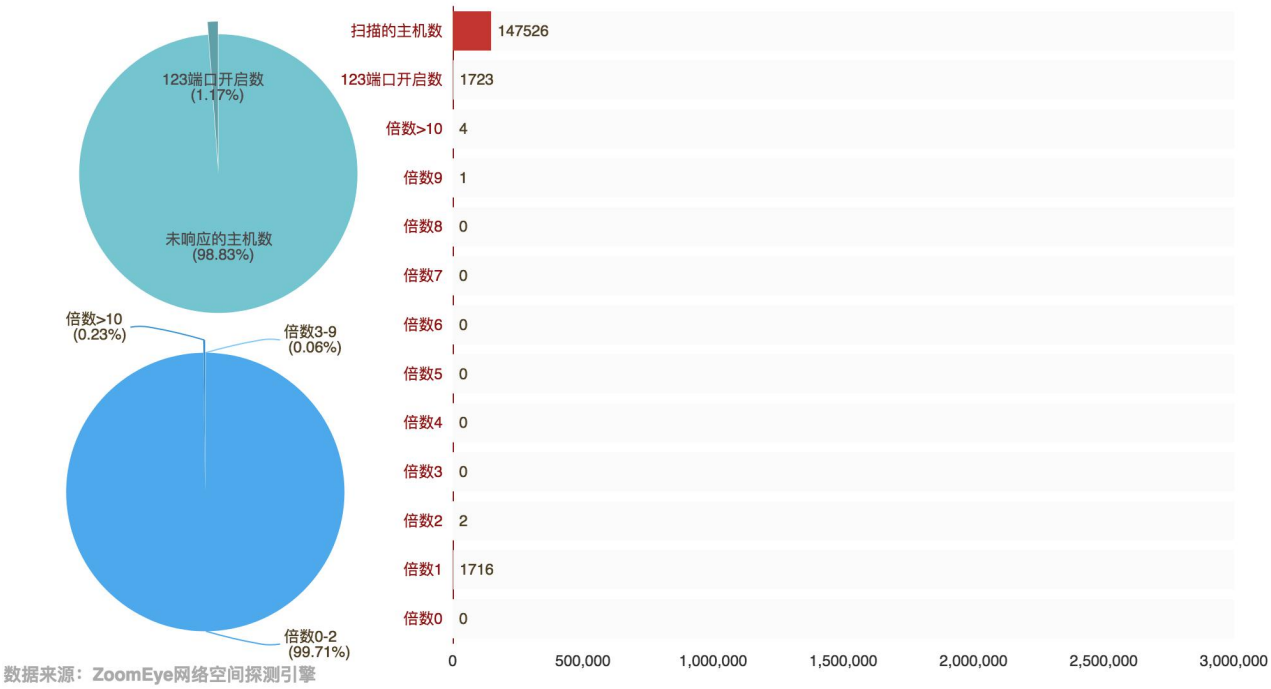


3-1.3 Chargen 协议 19 端口可利用主机全国分布图

3.2. NTP

通过 ZoomEye 网络空间探测引擎获取到 14 万(147,526)台开启了 UDP 123 端口的主机。利用这些数据进行放大倍率探测，实际上只有 1 千(1,723)台主机开启了 UDP 123 端口，占总数的 1.17%，放大倍数大于 10 的主机只有 4 台，占有响应主机总数的 0.23%，具体数量见图 3.2-1 所示：

3.2-1 NTP协议123端口探测统计图

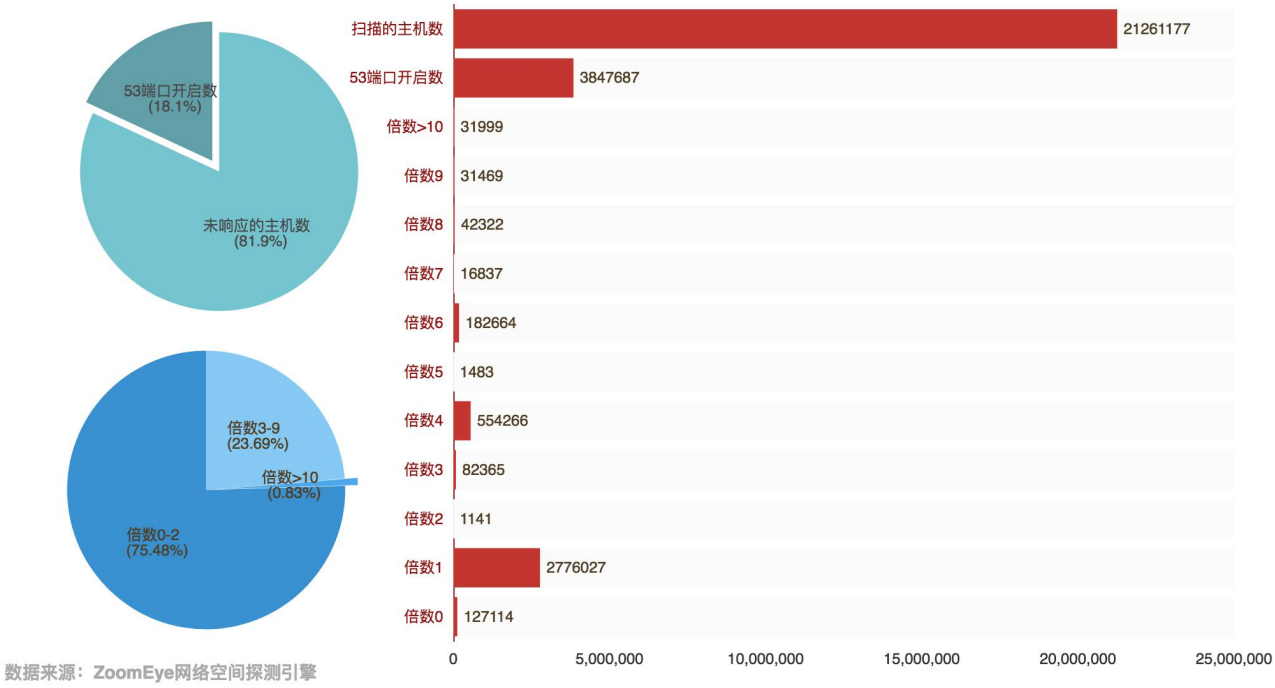


和上一次探测的结果相比，利用 NTP 进行反射 DDoS 攻击的隐患基本消除，不管是 NTP 服务器的总量还是可被利用服务器数量，都大幅度下降，尤其是本次探测中，只发现 4 台可被利用的 NTP 服务器，而且这 4 台皆位于日本。我国未被探测到可被利用的 NTP 服务器。

3.3. DNS

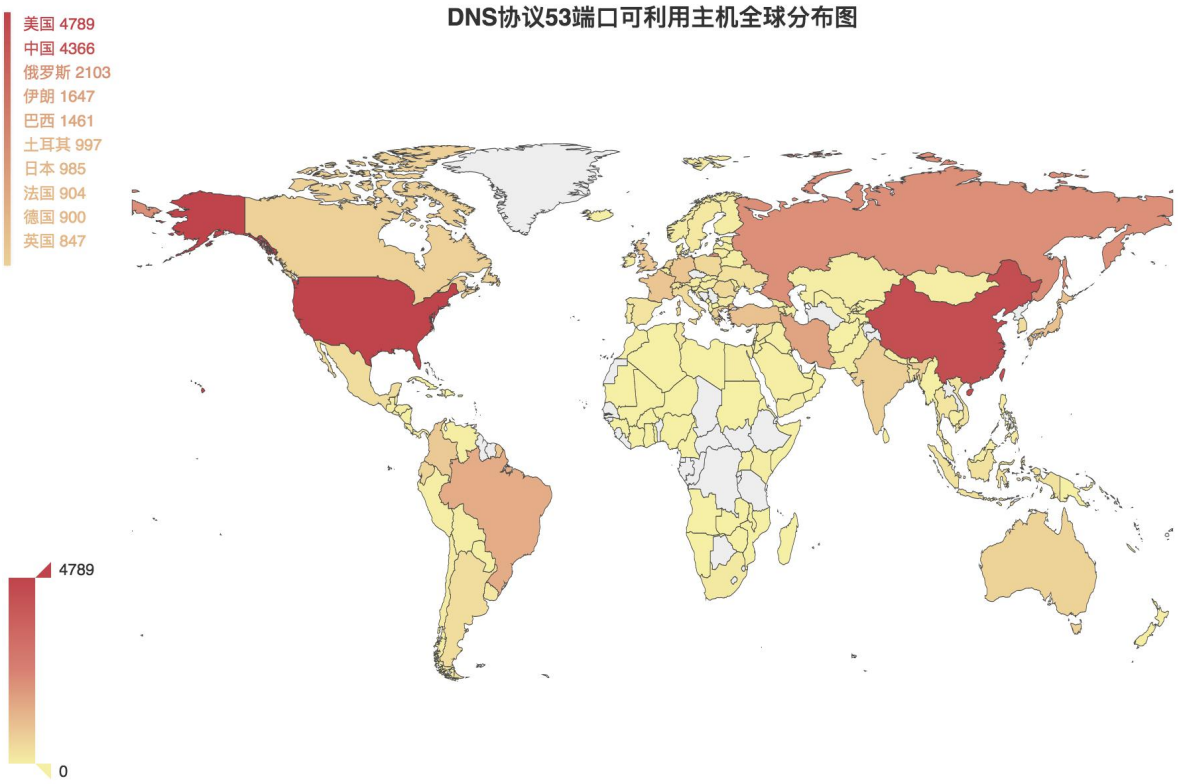
通过 Zoomeye 网络空间探测引擎获取到 2 千万(21,261,177)台 UDP 53 端口相关的主机，对这些主机进行放大倍率探测，实际上只有 384 万(3,847,687)台主机开启了 53 端口，占了扫描总数的 18.1%。在开启了 53 端口的主机中，有 3 万(31,999)台主机放大倍数在 10 倍以上，只占总数的 0.83%，而放大倍数为 1 的主机有 277 万(2,776,027)台，具体数据见图 3.3-1：

3.3-1 DNS协议53端口探测统计图

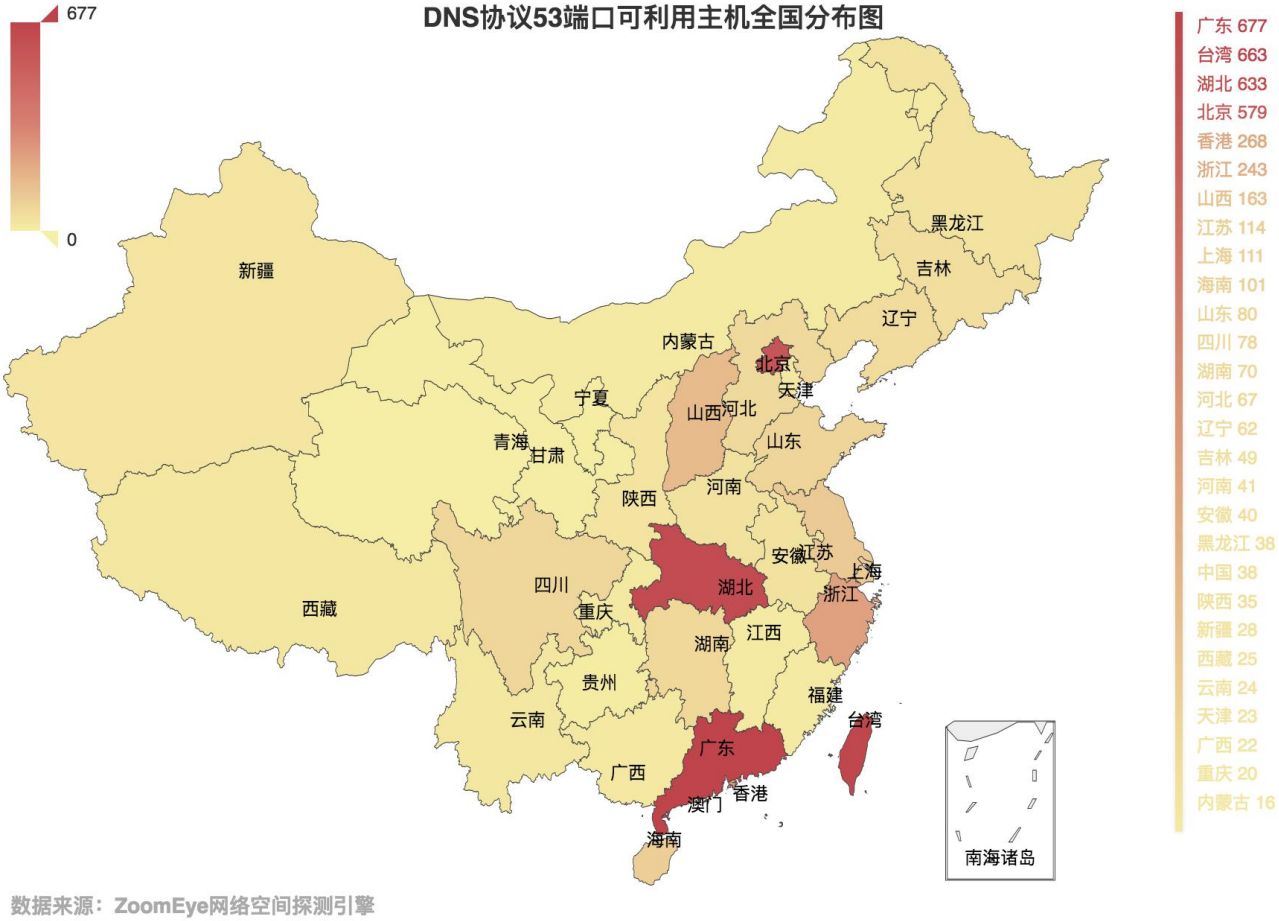


和上一版的数据相比，互联网上 DNS 服务器的和可被利用的 DNS 服务器数量均处于下降状态。

下面，再来看看这 3 万台放大倍数大于 10 的主机全球分布情况，如图 3.3-2 所示，可以看到，和上一轮相比，数量排名没啥变化，仍然是美国排在第一位。我们又对可利用主机在我国的分布情况进行了统计，如图 3.3-3 所示，和上一轮相比，湖北省的 DNS 服务器数量有了明显的提高。



3.3-2 DNS 协议 53 端口可利用主机全球分布图

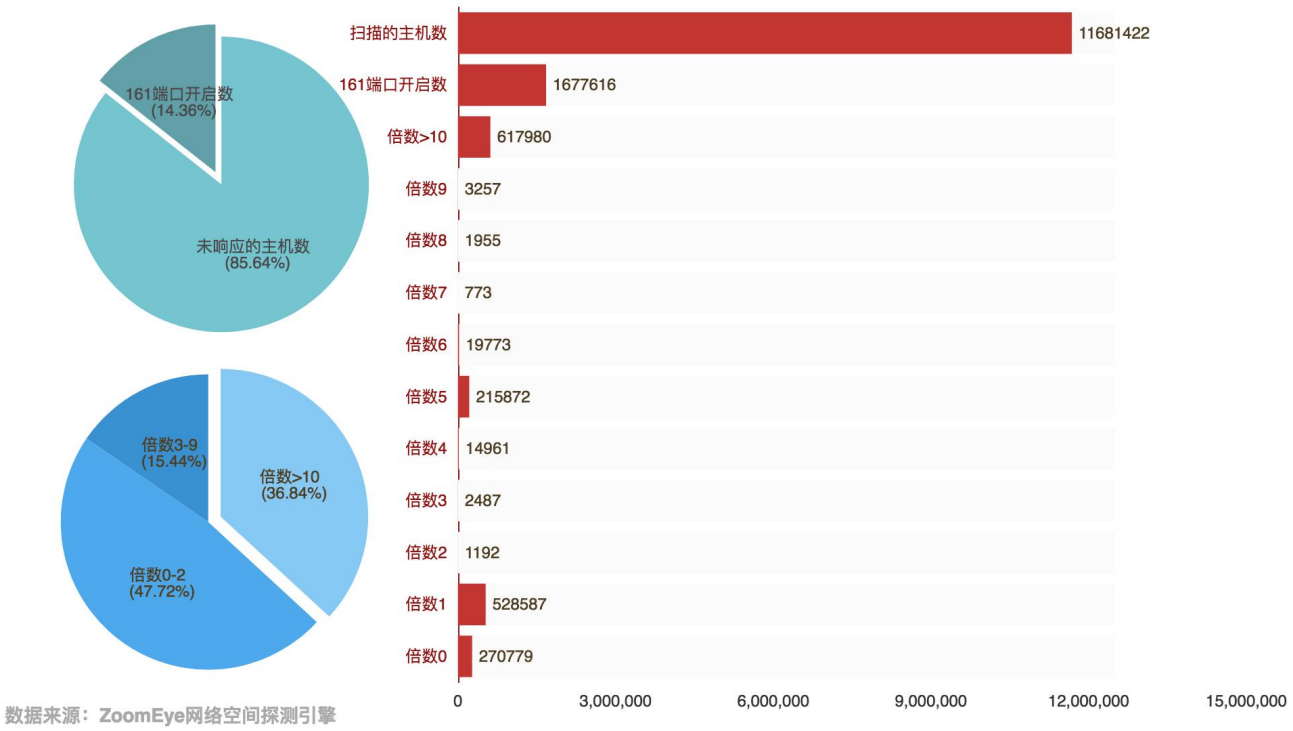


3.3-3 DNS 协议 53 端口可利用主机全国分布图

3.4. SNMP

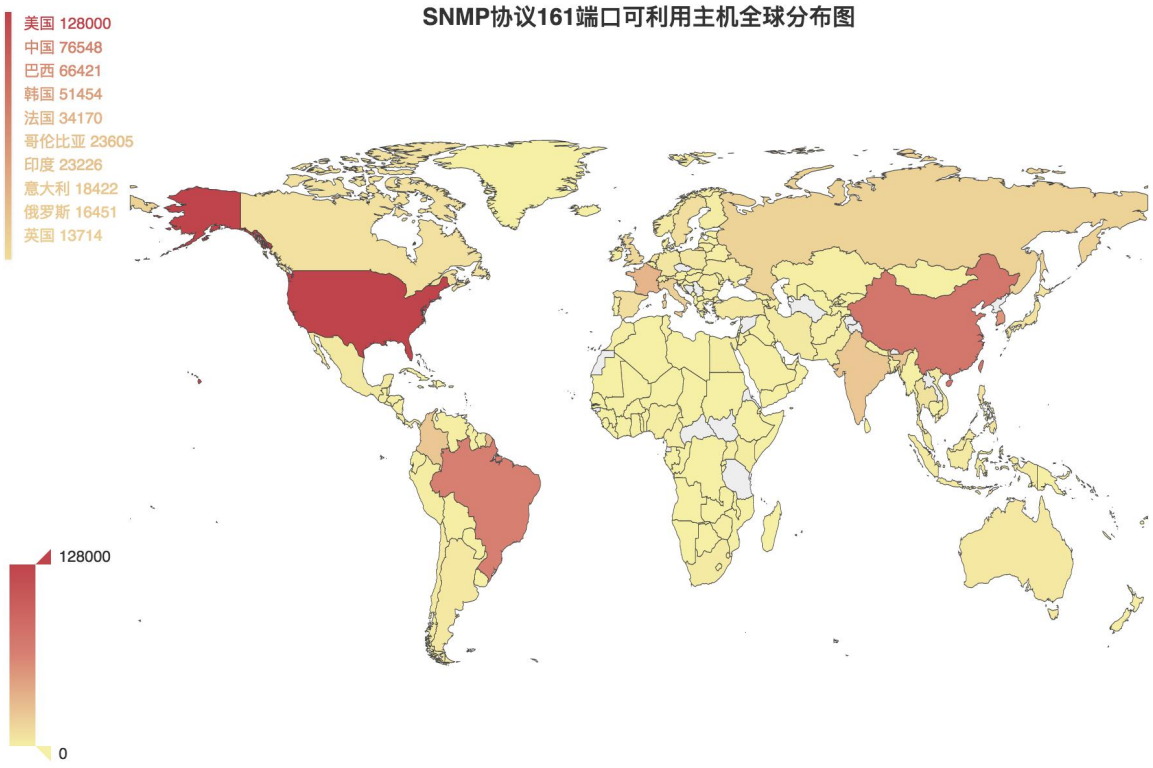
通过 Zoomeye 网络空间探测引擎获取到 1 千万(11,681,422)台 UDP 161 端口相关的主机，对这些主机进行放大倍率探测，实际上有 167 万(1,677,616)台主机开启了 161 端口，占了扫描总数的 14.36%。在开启了 161 端口的主机中，有 61 万(617,980)台主机放大倍数在 10 倍以上，占了总数的 36.84%，具体数据见图 3.4-1：

3.4-1 SNMP协议161端口探测统计图

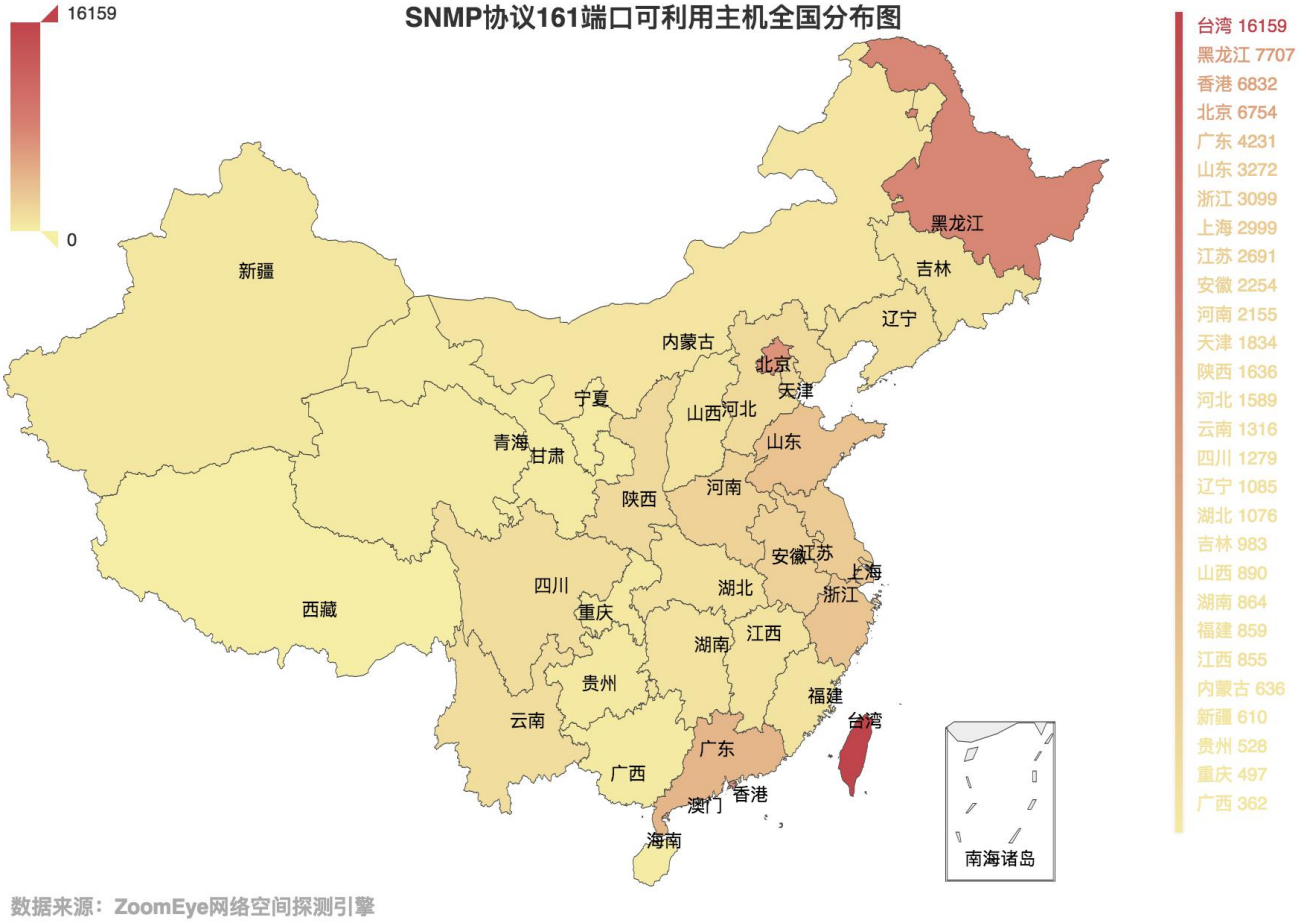


本次探测得到的数据和前一轮的数据相比较，探测到的 SNMP 主机数增加，而可利用的主机数却呈下降状态。

下面，再来看看这 61 万台放大倍数大于 10 的主机全球分布情况，如图 3.4-2 所示，可以看到，我国的主机量上升到了第二位。我们又对可利用主机在我国的分布情况进行了统计，如图 3.4-3 所示，台湾，北京，黑龙江仍然是受影响最深的几个省份之一。



3.4-2 SNMP 协议 161 端口可利用主机全球分布图

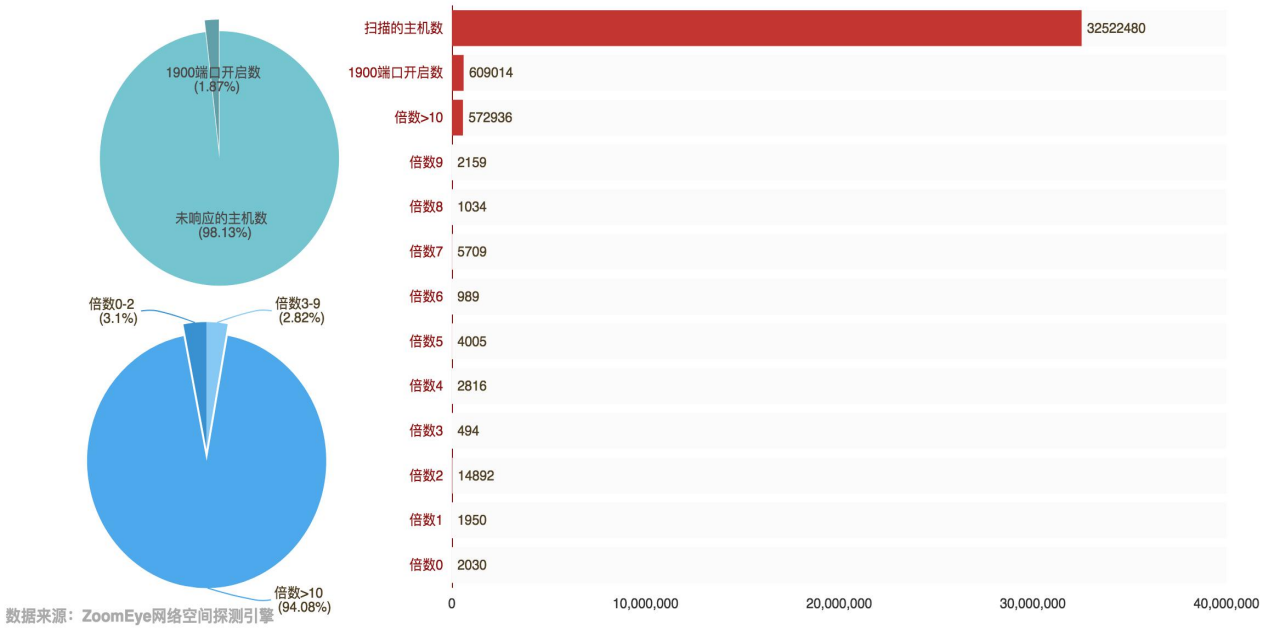


3.4-3 SNMP 协议 161 端口可利用主机全国分布图

3.5. SSDP

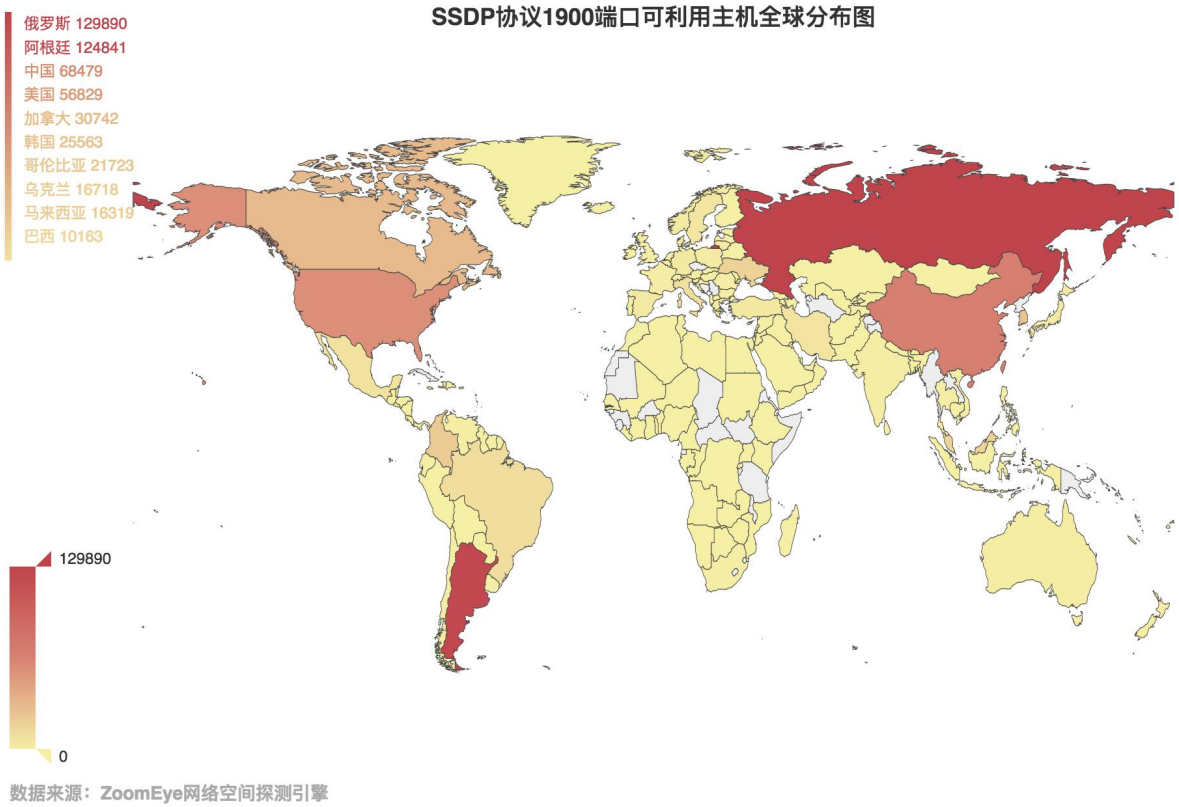
通过 Zoomeye 网络空间探测引擎获取到 3 千万(32,522,480)台 UDP 1900 端口相关的主机，对这些主机进行放大倍率探测，实际上有 60 万(609,014)台主机开启了 1900 端口，占了扫描总数的 1.87%。在开启了 1900 端口的主机中，有 57 万(572,936)台主机放大倍数在 10 倍以上，占了总数的 94.08%，具体数据见图 3.5-1：

3.5-1 SSDP协议1900端口探测统计图

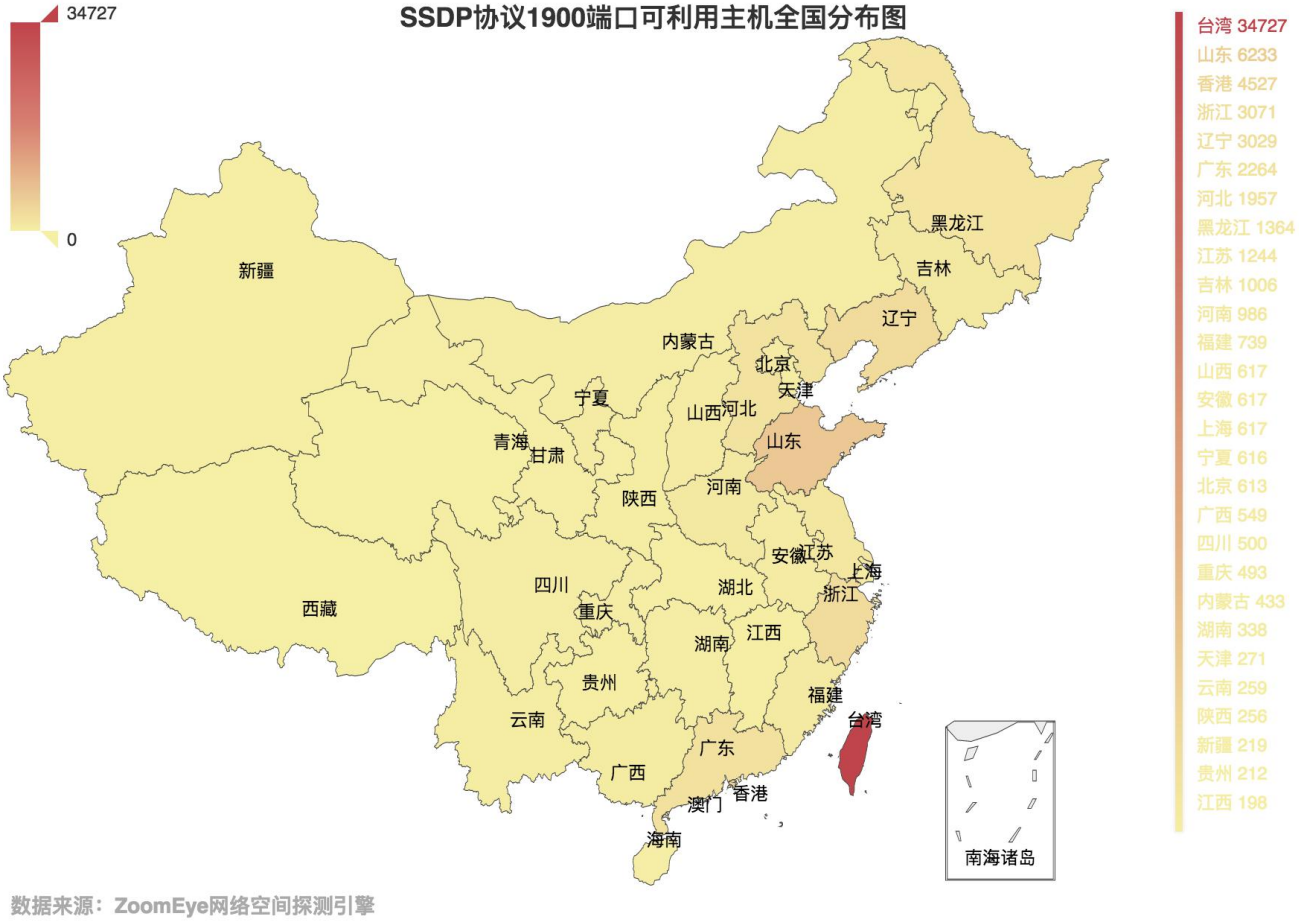


下面，再来看看这 57 万台放大倍数大于 10 的主机全球分布情况，如图 3.5-2 所示，和上一轮探测的数据相比，没有明显的变化。

再对我国的数据进行统计，如图 3.5-3 所示，台湾仍是我国可被利用的主机数最多的省份，远远超过我国的其他省份。



3.5-2 SSDP 协议 1900 端口可利用主机全球分布图

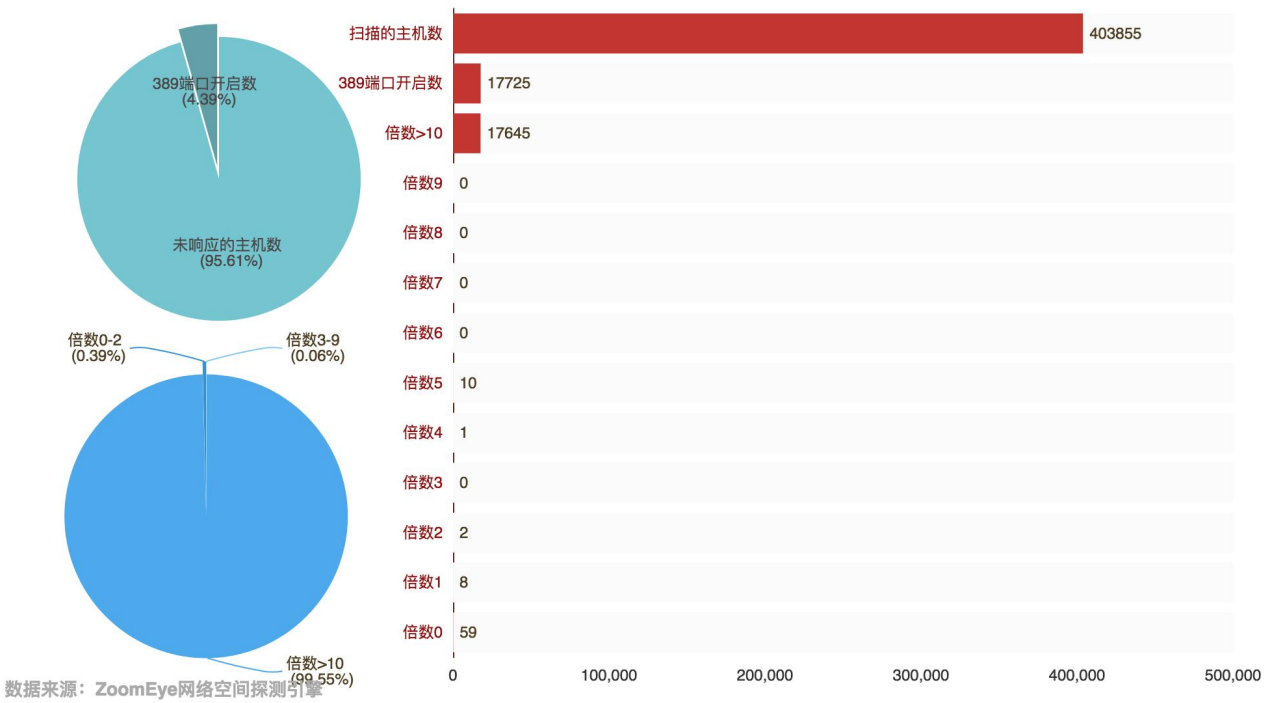


3.5-3 SSDP 协议 1900 端口可利用主机全国分布图

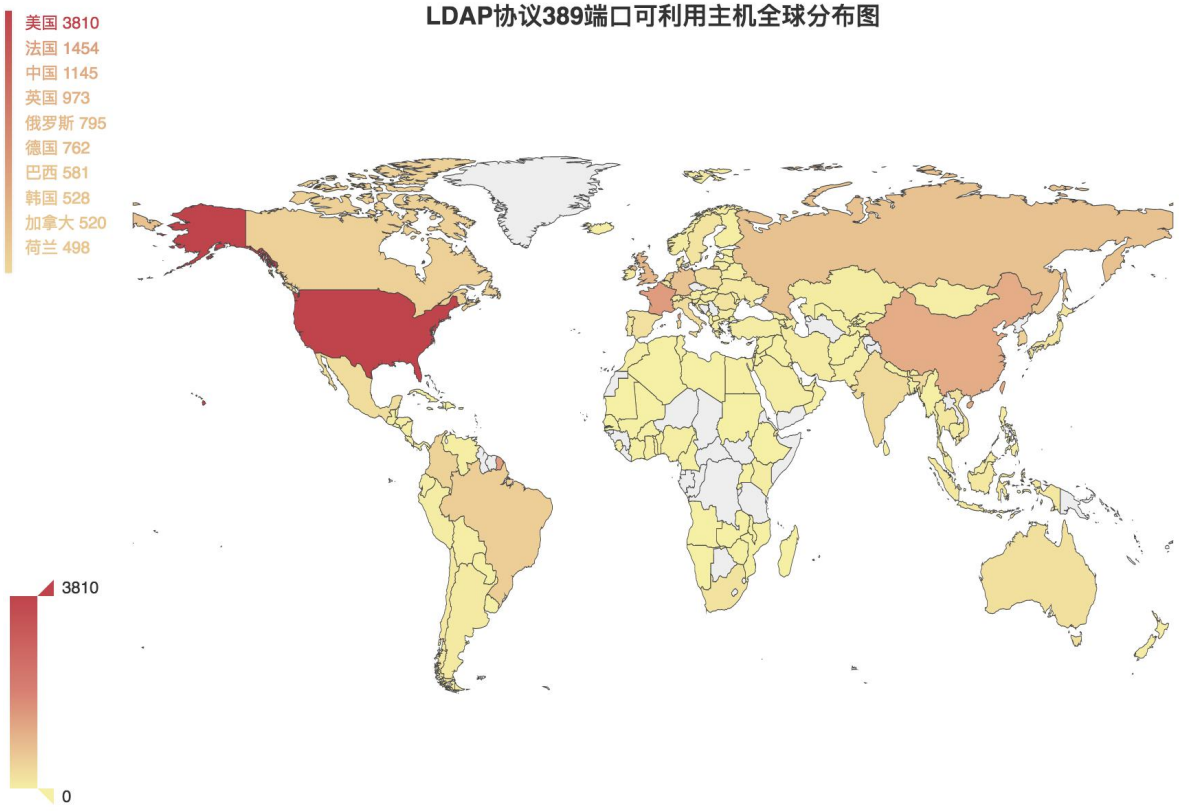
3.6. CLDAP

通过 Zoomeye 网络空间探测引擎获取到 40 万(403,855)台 UDP 389 端口相关的主机，对这些主机进行放大倍率探测，实际上有 1 万(17,725)台主机开启了 389 端口，占了扫描总数的 4.39%。在开启了 389 端口的主机中，有 1 万(17,645)台主机放大倍数在 10 倍以上，占了总数的 99.55%，具体数据见图 3.6-1：

3.6-1 LDAP协议389端口探测统计图



下面，再来看看这 2 万台放大倍数大于 10 的主机全球分布情况，如图 3.5-2 所示，可以看到，美国仍然是可被利用的 CLDAP 服务器数量最多的国家，我国依旧排第三位。我们又对可利用主机在我国的分布情况进行了统计，如图 3.5-3 所示，台湾依然是我国可被利用的主机数最多的省份，和香港一起远远超过我国的其他省份地区。



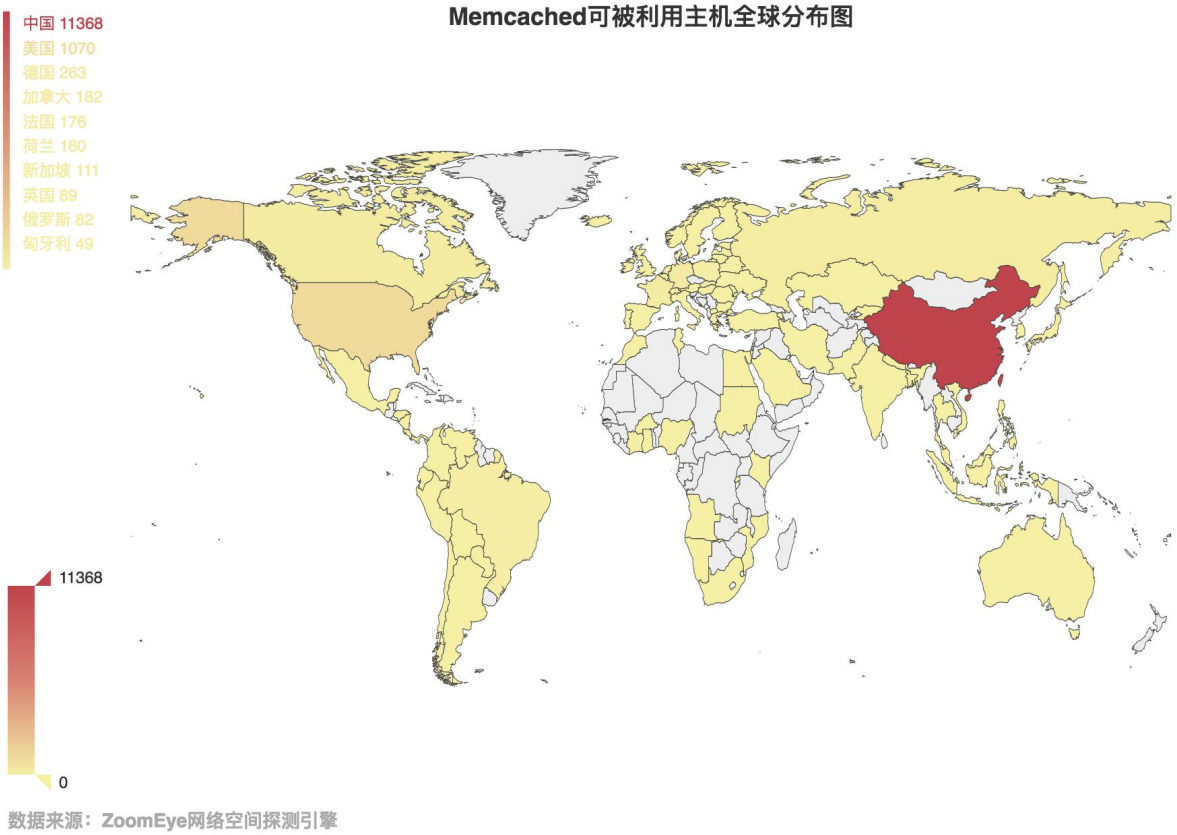
3.6-2 LDAP 协议 389 端口可利用主机全球分布图

3.6-3 LDAP 协议 389 端口可利用主机全国分布图

3.7. Memcached

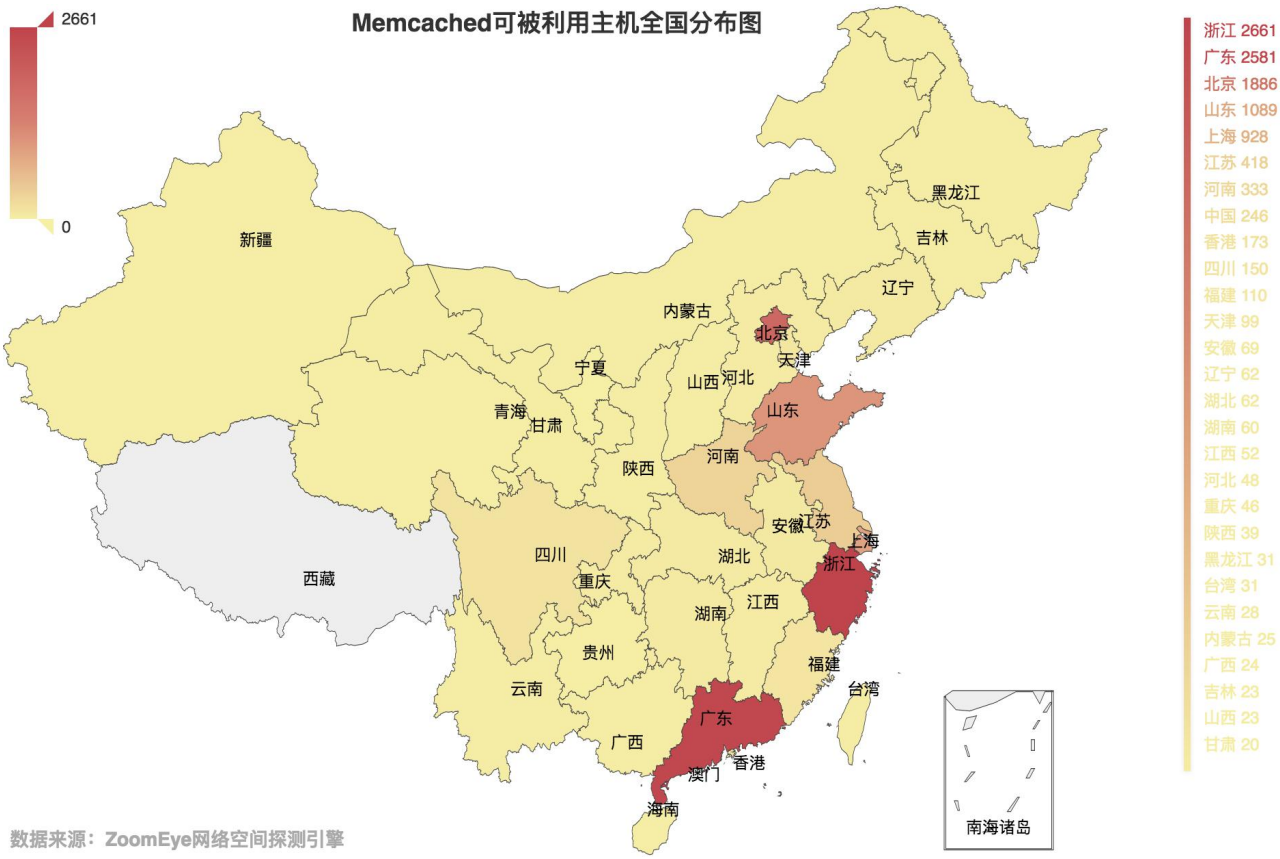
Memcached 是一个自由开源的，高性能，分布式内存对象缓存系统。Memcached 是以 LiveJournal 旗下 Danga Interactive 公司的 Brad Fitzpatric 为首开发的一款软件。现在已成为 mixi、hatena、Facebook、Vox、LiveJournal 等众多服务中提高 Web 应用扩展性的重要因素。Memcached 是一种基于内存的 key-value 存储，用来存储小块的任意数据（字符串、对象）。这些数据可以是数据库调用、API 调用或者是页面渲染的结果。Memcached 简洁而强大。它的简洁设计便于快速开发，减轻开发难度，解决了大数据量缓存的很多问题。它的 API 兼容大部分流行的开发语言。本质上，它是一个简洁的 key-value 存储系统。一般的使用目的是，通过缓存数据库查询结果，减少数据库访问次数，以提高动态 Web 应用的速度、提高可扩展性。

Memcached Server 在默认情况下同时开启了 TCP/UDP 11211 端口，并且无需认证既可使用 Memcached 的储存服务。2018 年 3 月 2 日，ZoomEye 对全网开启了 UDP 11211 端口，并且无需认证的 Memcached 进行探测，共得到 14142 个目标，并对这些目标进行全球分布统计，如图 3.7-1 所示：



3.7-1 Memcached 可被利用主机全球分布图

从上图中可以明显的看出我国对安全问题的重视程度和国外仍然有较大的差距。在 14142 个有效目标中，有 11368 个目标的 IP 地址位于我国。下面再对我国的目标进行全国分布统计，如图 3.7-2 所示：

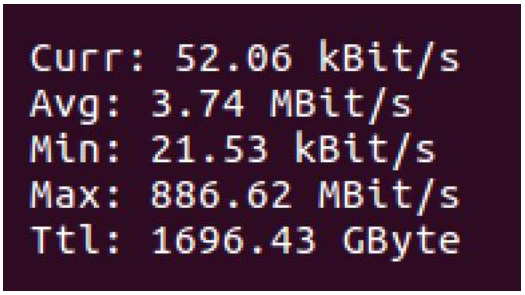


3.7-2 Memcached 可被利用主机全国分布图

Memcached 未开启认证的情况下，任何人都可以访问 Memcached 服务器，储存键值对，然后可以通过 key 来获取 value。所以，我们能在 Memcached 储存一个 key 为 1byte 的，value 为 1kb 的数据，然后我们再通过该 key 获取到 value，这样就产生了将近 1000 倍的放大效果。Memcached 在默认情况下还会开启 UDP 端口，所以这就导致了 Memcached 可以被利用来进行 DDoS 放射放大攻击。而 Memcached 能放大多少倍取决于：

1. Memcached 服务器带宽
2. Memcached 能储存的值的最大长度

利用自己的服务器进行一个测试，首先让能利用的 Memcached 储存一个 1kb 长度的值，然后同时向所有目标获取值，能收到 886Mbit/s 的流量，如图 3.7-3 所示：



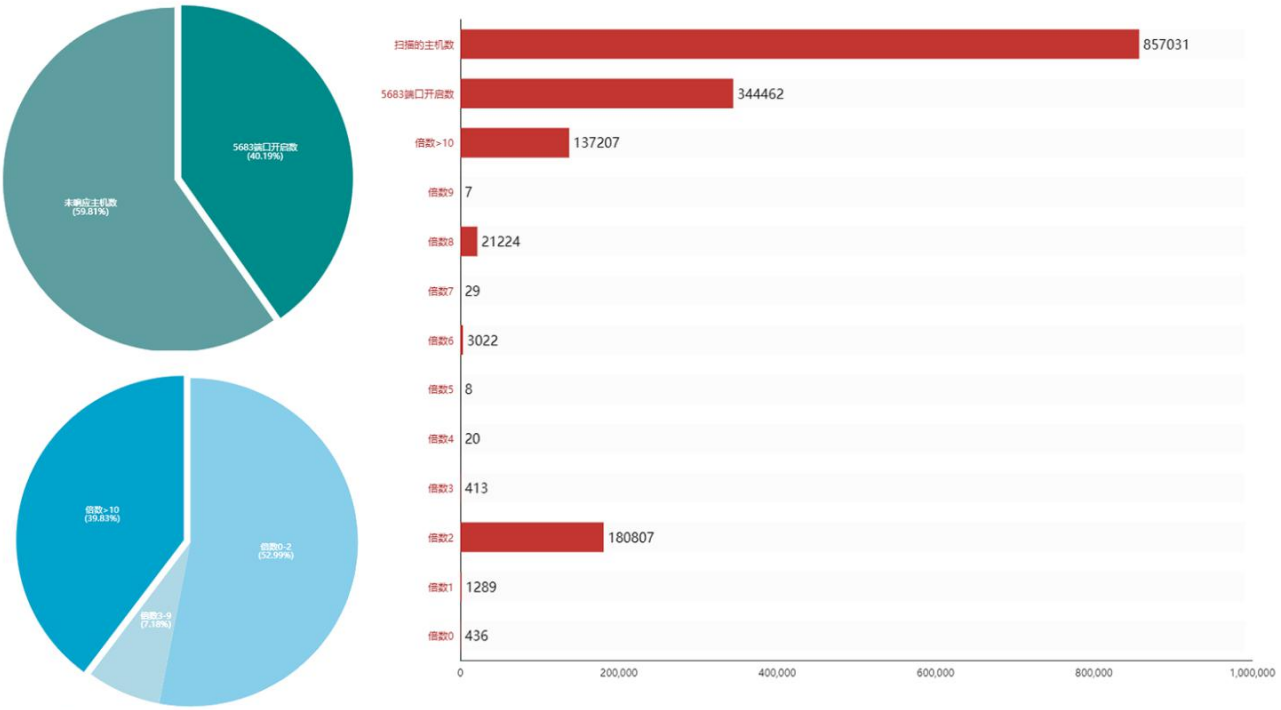
3.7-3 流量统计图

3.8. CoAP

CoAP（Constrained ApplicationProtocol）是一种应用在物联网网络的应用层协议，它的详细规范定义在 RFC 7252。由于物联网设备大多都是资源限制型设备，例如有限的 CPU、RAM、带宽等。对于这类设备来说想要直接使用现有网络的 TCP 和 HTTP 来实现设备间的通信显得很奢侈。为了让这部分资源受限的设备也能够顺利的接入网络，CoAP 协议应运而生。CoAP 指受限制的应用协议，是基于 UDP 实现的类 HTTP 协议。相比于 HTTP 协议，CoAP 继承了 HTTP 协议的可靠传输，数据重传，块重传，IP 多播等特点。并且 CoAP 利用二进制格式传递数据，这样使得 CoAP 请求更加的轻量化，并且占用的带宽更小。

CoAP 协议规定提供服务的设备，必须提供./well-known/core 的 Uri-path 并且默认绑定在 5683 端口上。2019 年 5 月 6 日，通过 Zoomeye 网络空间探测引擎获取到 857,031 台 UDP 5683 端口相关的主机，对这些主机进行放大倍率探测，实际上有 344,462 台主机开启了 5683 端口，占了扫描总数的 40.19%。在开启了 5683 端口的主机中，有 137,207 台主机放大倍数在 10 倍以上，占了总数的 39.83%，具体数据见图 3.8-1：

3.8-1 CoAP协议5683端口探测统计图



数据来源: ZoomEye网络空间探测引擎

对响应主机全球分布情况分析如图 3.8-2，可以看到主要分布在俄罗斯与中国：

3.8-2 CoAP 可被利用主机全球分布图

对响应主机国内分布情况分析如图 3.8-3，主要分布在江西、四川、新疆

3.8-3 CoAP 可被利用主机全国分布图

另外，我们对国内设备的响应报文进行了简单分析，发现有大量设备的响应数据中都包含有 Qlink 关键字。

4. 总结

和前面三轮探测的数据相比，在第四轮的探测中，变化最大的是 NTP 服务，当前互联网的 NTP 服务器已经没办法造成大流量的 DDoS 反射放大攻击了。与之相比，其他协议也或多或少的降低了可被利用的主机数量 。DDoS 反射放大攻击仍然危害巨大，DDoS 防御仍然刻不容缓。

对于 Memcached，从 ZoomEye 探测到的数据中，再和公网上的 Memcached 服务进行对比：

4-4 ZoomEye 探测 11211 端口数量

在 ZoomEye 的数据库中，开启 11211 端口的目标有 54 万，其中美国有 23 万，中国有 13 万的目标，但是开启了 UDP 11211 端口的数据中，总量只有 14142，其中美国有 1070 的目标，中国有 11368 个目标主机。

从这些数据对比中，可以看出美国对此类的安全事件有非常快的响应速度，中国和美国的差距还很大。

从放大效果来看，虽然可利用的目标已经缩减到 1 万的量级，但是仍然能造成大流量的 DDos 攻击。

对于 Memcached 的用户，我们建议关闭其 UDP 端口，并且启用 SASL 认证，对于运营商，建议在路由器上增加的 uRPF(Unicast Reverse Path Forwarding)机制，该机制是一种单播反向路由查找技术，用于防止基于源地址欺骗的网络攻击行为，利用该机制能使得 UDP 反射攻击失效。

第五版中，增加了对于 CoAP 的探测，从上面统计与分析的数据中可以看到，能被利用进行 DDoS 反射放大的主机主要分布在俄罗斯与中国，并且放大效果在 10 倍以上的主机也不少。对于使用 CoAP 的互联网服务，可以禁用 UDP，不能禁用时确保请求与响应不要有倍数关系，也可以启用授权认证；对于企业用户，没有 UDP 相关业务，可以再上层或者本机防火墙过滤掉 UDP 包，可以寻求运营商提供 UDP 黑洞的 IP 网段做对外网站服务，也可以选择接入 DDoS 云防安全服务或删除协议默认路径；对物联网用户，如果没有公网访问需求，物联网设备不启用公网 IP，如果有公网访问需求，应添加防火墙规则，限制访问 IP，减少互联网暴露面。

5. 参考链接

1. Stupidly Simple DDoS Protocol (SSDP) generates 100 Gbps DDoS.
https://blog.cloudflare.com/ssdp-100gbps/
2. 基于 SNMP 的反射攻击的理论及其实现.
http://drops.xmd5.com/static/drops/tips-2106.html
3. 基于 Memcached 分布式系统 DRDoS 拒绝服务攻击技术研究.
https://paper.seebug.org/535/
4. ZoomEye Chargen dork.
https://www.zoomeye.org/searchResult?q=port%3A19
5. ZoomEye NTP dork.
https://www.zoomeye.org/searchResult?q=port%3A123
6. ZoomEye DNS dork.
https://www.zoomeye.org/searchResult?q=port%3A53
7. ZoomEye SNMP dork.
https://www.zoomeye.org/searchResult?q=port%3A161
8. ZoomEye LDAP dork.
https://www.zoomeye.org/searchResult?q=port%3A389
9. ZoomEye SSDP dork.
https://www.zoomeye.org/searchResult?q=port%3A1900
10. ZoomEye Memcached dork.
https://www.zoomeye.org/searchResult?q=port%3A11211
11. ZoomEye CoAP dork
https://www.zoomeye.org/searchResult?q=port%3A5683