知道创宇 KNOWNSEC.COM ZoomEye

Global Detection and Analysis of Amplified Reflection DDoS Attacks

V 5.0

May 6th, 2019

Knownsec 404 Team

1. Updates

Version	Date	Description
V1.0	2017/08/07	Complete the first round of data statistics
V2.0	2017/08/14	Complete the second round of data statistics
V3.0	2017/11/15	Complete the third round of data statistics, and increase data detection for CLDAP
V4.0	2018/03/05	Complete the fourth round of data statistics, and increase data detection for Memcached
V5.0	2019/05/06	On the basis of the fourth round of data statistics, increase the detection of CoAP, and perfect for the fifth edition

2. Overview

DDoS attack is a type of network attack that runs out of resources. Through the high-traffic attacks and targeted exploits, attackers exhaust the resources of the host computers to achieve the purpose of the denial of service.

The amplified reflection attack is a DDoS attack method with great power. The attacker only needs to pay a little to generate huge traffic for the target, thus causing tremendous pressure on the network bandwidth resources (network layer), connection resources (transport layer), and computer resources (application layer).

In October 2016, Dyn's DNS server suffered a DDoS attack, which caused a large-scale disconnection of network in the United States. The analysis showed that the DNS amplified reflection attack and the SYN flood attack were the main force of this denial-of-service attack that caused the U.S. to disconnect the network. As amplified reflection attack is harmful, low-cost and difficult to trace the source, it has been widely used in network black industry chain.

From August 3rd, 2017 to August 6th, 2017, the ZoomEye cyberspace detection engine performed the first round of detection on the entire network, counted the number of hosts that can be exploited for amplified reflection DDoS attacks, then released "Global Detection and Analysis of Amplified Reflection DDoS Attacks - V1.0".

From August 11th, 2017 to August 13th, 2017, ZoomEye probed the entire network once again and released the "Global Detection and Analysis of Amplified Reflection DDoS Attacks - V2.0".

From November 13th, 2017 to November 15th, 2017, ZoomEye detected another active attack-- the CLDAP amplified reflection DDoS attack. After the third round of detection, "Global Detection and Analysis of Amplified Reflection DDoS Attacks - V3.0" was released.

On March 1st, 2018, ZoomEye detected the frequent activity of Memcached DRDoS in cyberspace, and performed the fourth round of detection of amplified reflection DDoS attacks.

On May 6th, 2019, ZoomEye detected the frequent activity of CoAP DRDoS in cyberspace, and performed DDoS attack detection on CoAP, perfect the fifth edition.

3. The fifth edition data analysis of amplification attacks

[Note: The following statistics are based on the fourth round data 2018/03/05 and 2019/05/06]

On March 5, 2018, In the fourth round of detection, the ZoomEye cyberspace detection engine increased the detection of Memcached attacks based on the first two rounds.

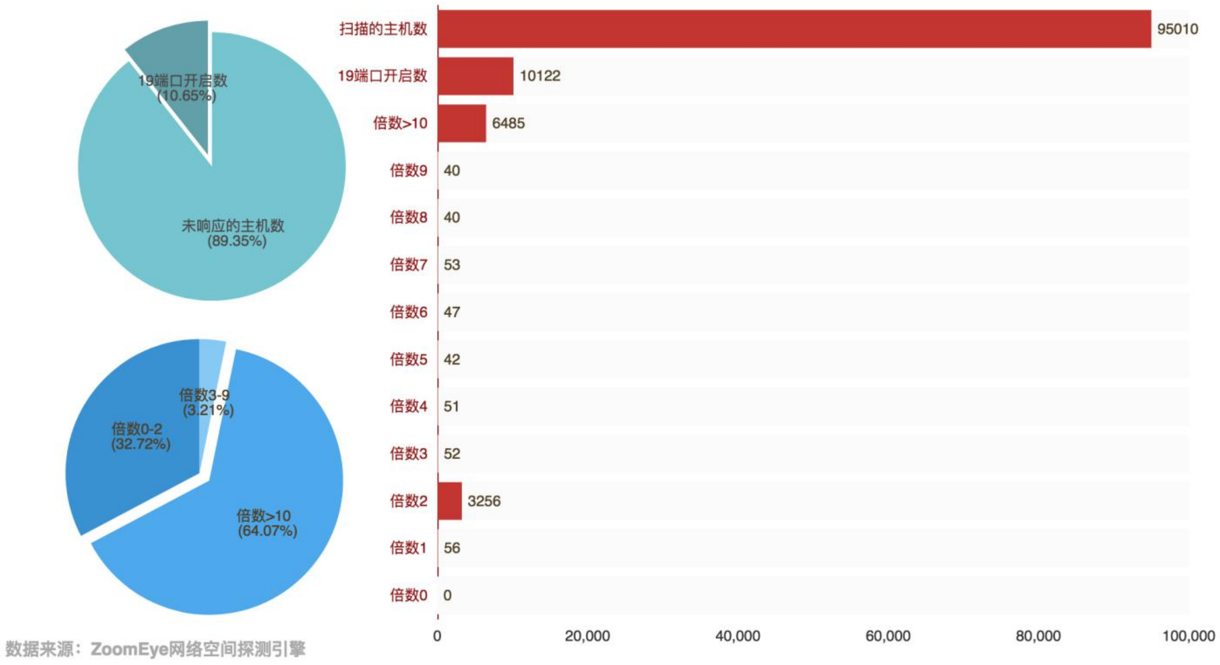
On May 6, 2019, the ZoomEye cyberspace detection engine increased the detection of CoAP based on the fourth round of statistics, perfect the fifth edition.

3.1. CHARGEN

Through the data obtained by the ZoomEye cyberspace detection engine, 95,010 hosts opened port 19. Then perform magnification detection of these hosts, in fact, only 10,122 hosts opened port 19, accounting for 10.65% of the total.

Among the hosts with port 19 open, 6,485 hosts can achieve more than 10 times the magnification, accounting for 64.07% of the total, the remaining hosts is mainly concentrated at 2 times. The relevant data are as follows:

3.1-1 Chargen协议19端口探测统计图

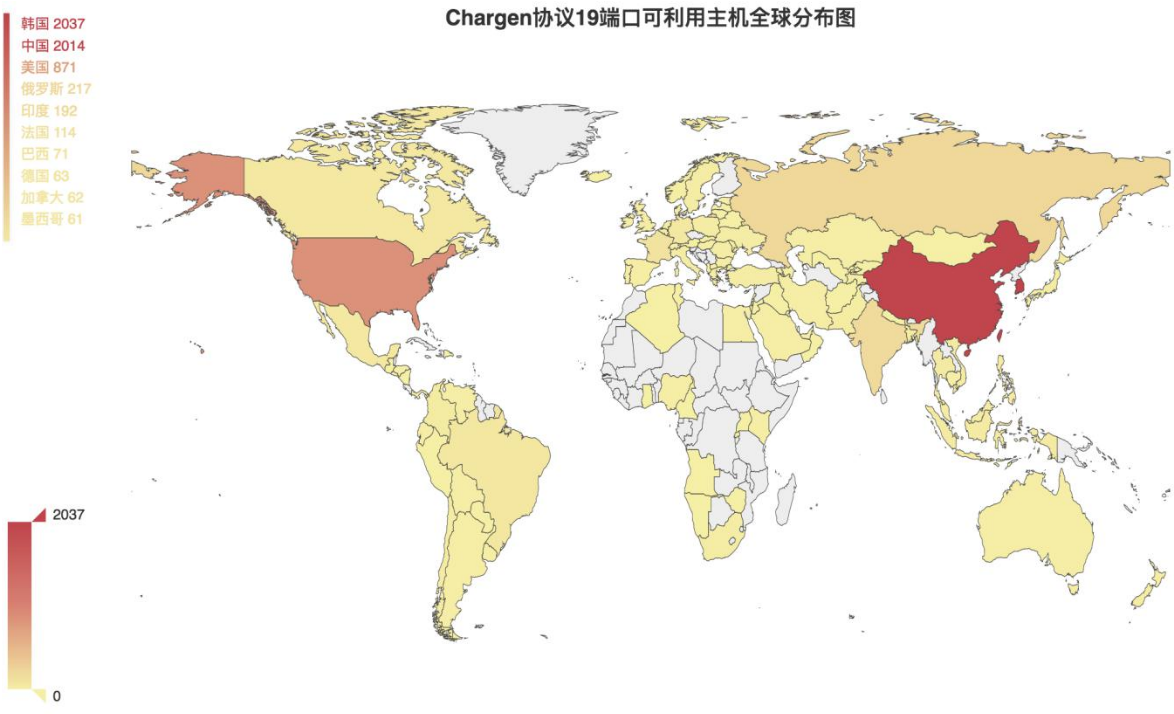


数据来源：ZoomEye网络空间探测引擎

For the statistics of the host traffic with a magnification of 10 or more, we sent a total of 870KB (891,693 bytes) of request traffic, and obtained 71M (74,497,401 byte) response traffic, resulting in 83 times of amplified traffic. Suppose a host can successfully respond to 100 request packets within 1 minute, the calculated attack traffic is 947 Mbits/s. This round of detection has been used to count the maximum magnification, and the Chargen protocol can achieve a maximum of 319 times the flow rate with a single request response.

Comparing the above data with the previous two, the harm of the Chargen DDoS attack has not decreased, but has an increasing trend.

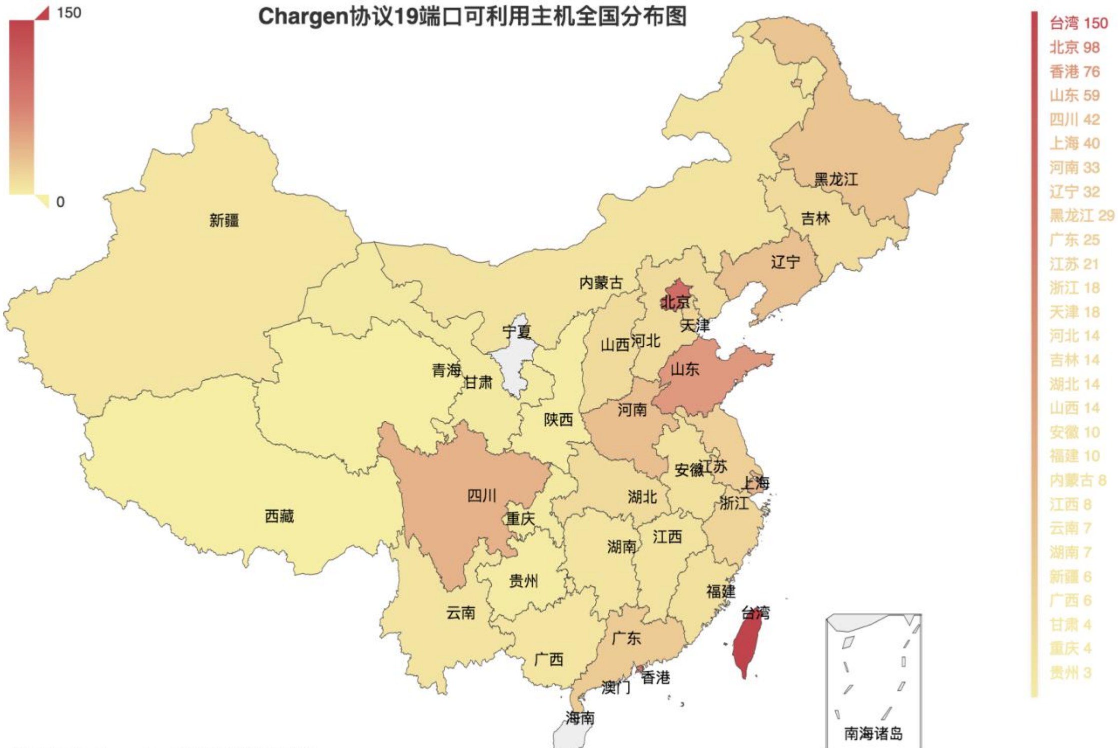
Based on the detection results of the ZoomEye cyberspace detection engine, we performed the global distribution statistics of available Chargen hosts:



数据来源：ZoomEye网络空间探测引擎

3.1-2 Global distribution map of Chargen protocol port 19 available hosts

It can be seen from the figure that Korea still has the largest number of hosts that can be used for amplified reflection DDoS attacks. China ranks second. Here, the statistics of the provinces in China are as shown in Figure 3.1-3:



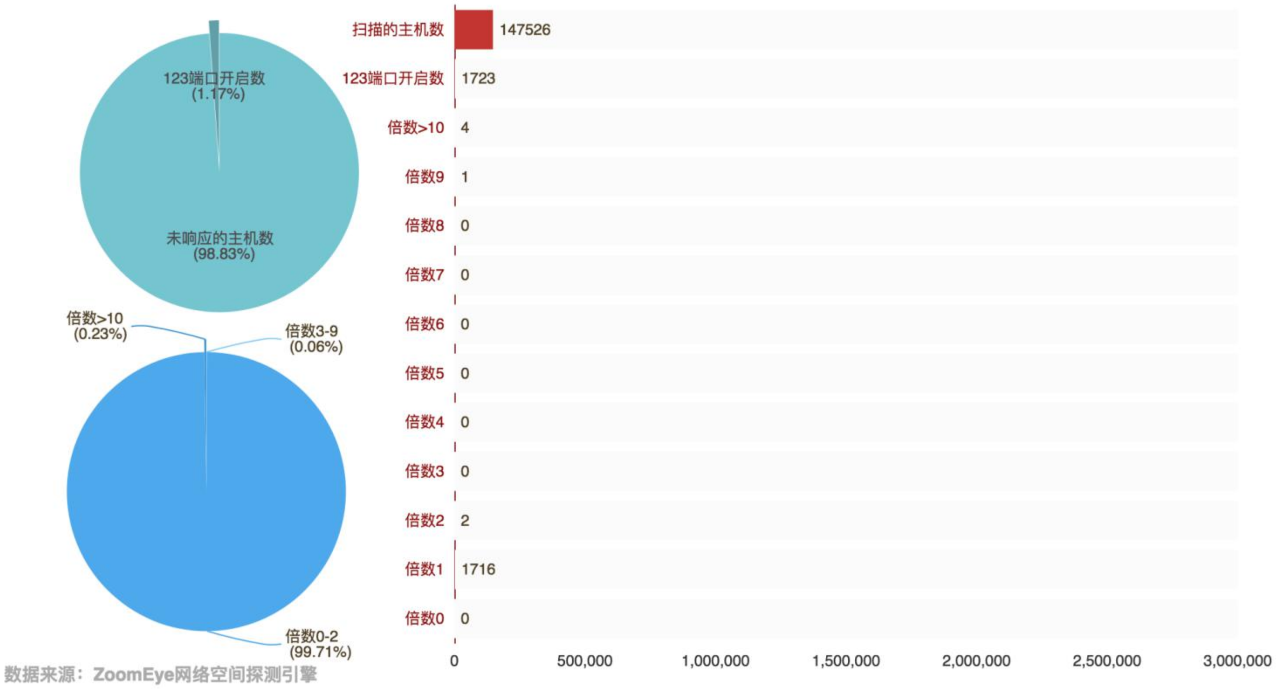
数据来源：ZoomEye网络空间探测引擎

3-1.3 Distribution map of Chargen protocol port 19 available hosts in China

3.2. NTP

Through the data obtained by the ZoomEye cyberspace detection engine, 147,526 hosts opened the UDP port 123. Then perform magnification detection of these hosts, in fact, only 1,723 hosts opened UDP port 123, accounting for 1.17% of the total. Only 4 hosts with a magnification greater than 10, which account for 0.23% of the total number of responding hosts. The specific data is as follows:

3.2-1 NTP协议123端口探测统计图



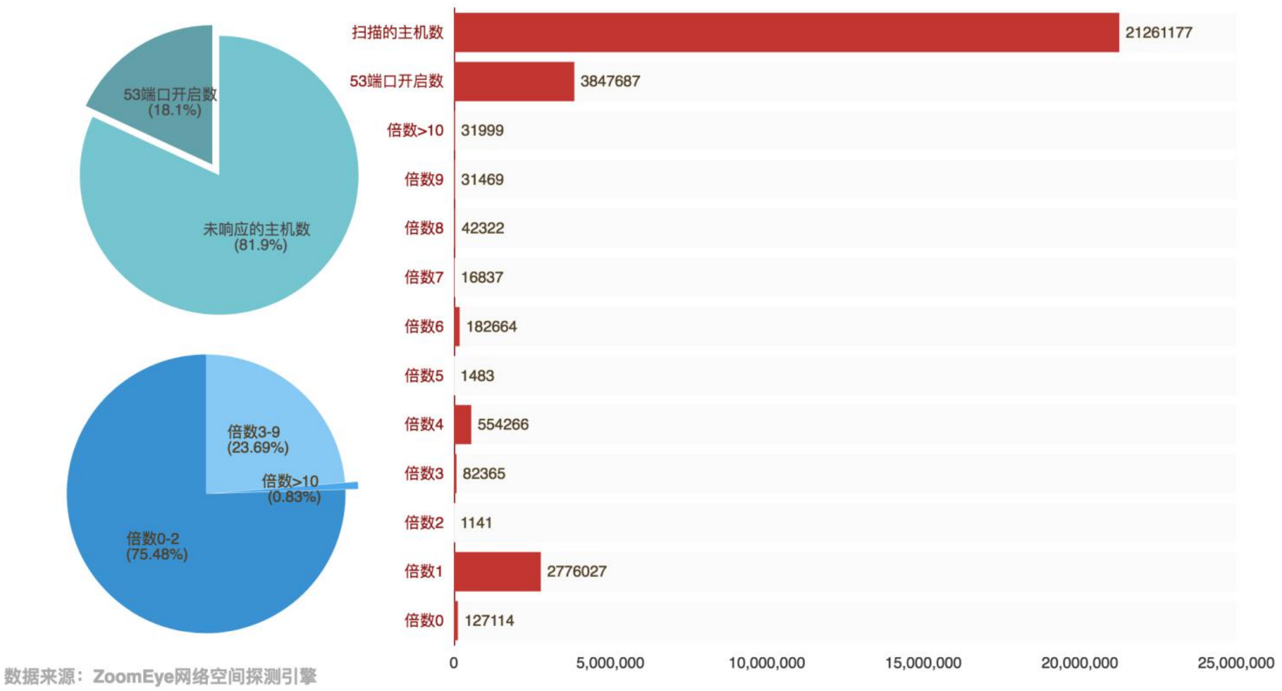
数据来源：ZoomEye网络空间探测引擎

Compared with the results of the previous detection, the hidden dangers of using NTP to perform DDoS attacks are basically eliminated. The total number of NTP servers and the number of servers that can be used are greatly reduced. Especially in this detection, only four NTP servers that can be used are found, and all four are located in Japan. China has not detected an NTP server that can be utilized.

3.3. DNS

Through the data obtained by the ZoomEye cyberspace detection engine, there are 21,261,177 hosts that related to the UDP port 53. Then perform magnification detection of these hosts, in fact, only 3,847,687 hosts opened port 53, accounting for 18.1% of the total number. Among the hosts with port 53 turned on, there are 31,999 hosts with a magnification of more than 10 times, accounting for only 0.83% of the total, 2,776,027 hosts with a magnification of 1. The specific data is as follows:

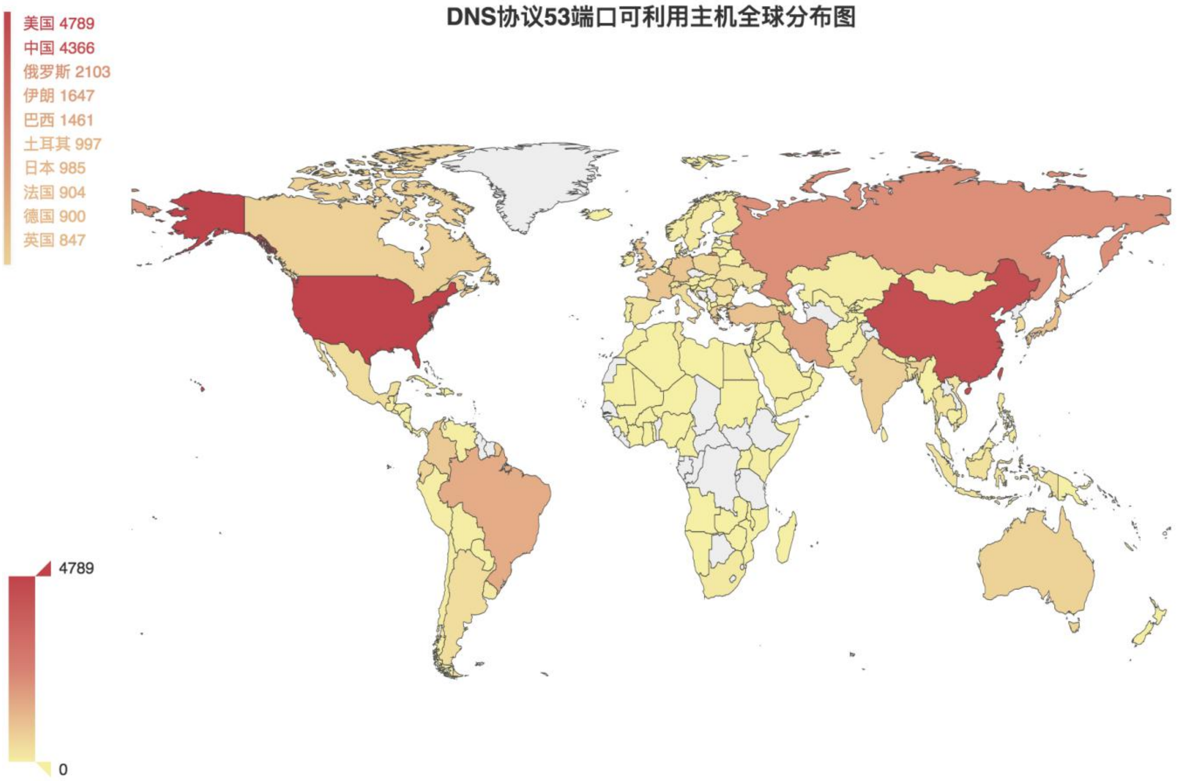
3.3-1 DNS协议53端口探测统计图



数据来源：ZoomEye网络空间探测引擎

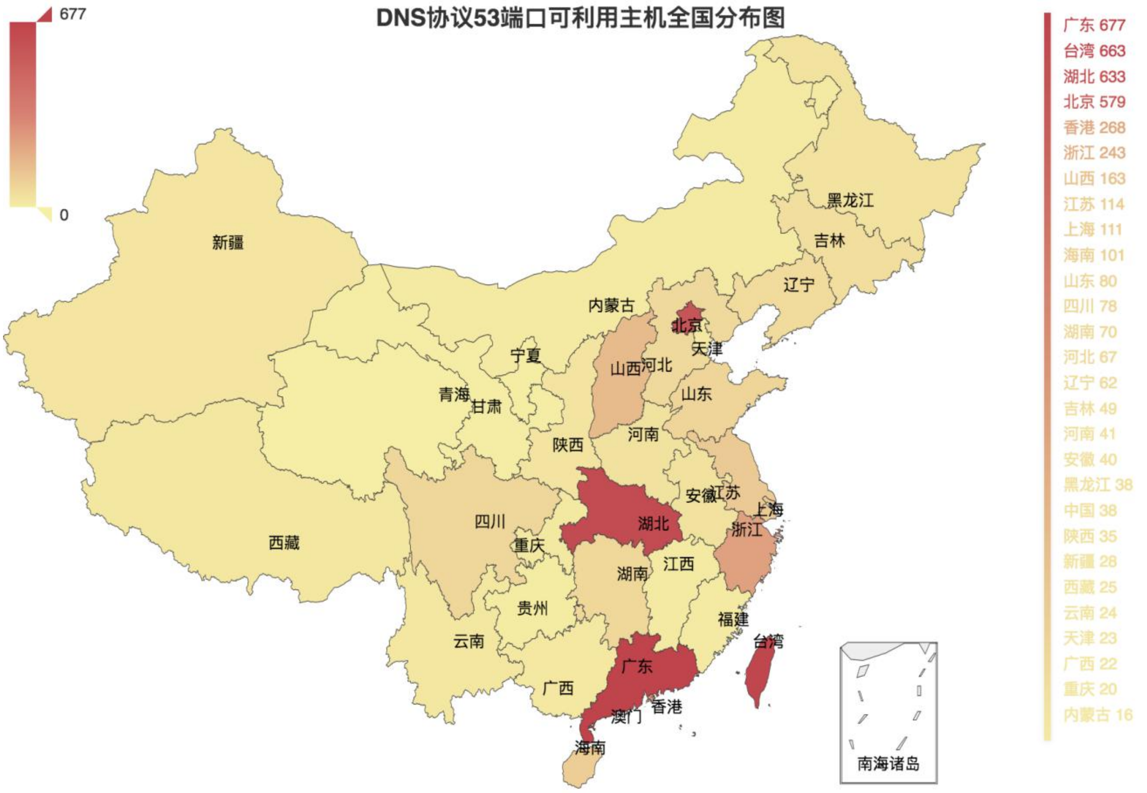
Compared with the previous version of the data, the number of DNS servers on the Internet and the number of DNS servers that can be utilized are declining.

Let's take a look at the global distribution of these hosts with a magnification greater than 10, as shown in Figure 3.3-2. It can be seen that compared with the previous round, the number ranking has not changed, and the US is still ranked the first one. We also made statistics on the distribution of available hosts in China, as shown in Figure 3.3-3. Compared with the previous rounds, the number of DNS servers in Hubei Province has been significantly improved.



数据来源：ZoomEye网络空间探测引擎

3.3-2 Global distribution map of DNS protocol port 53 available hosts



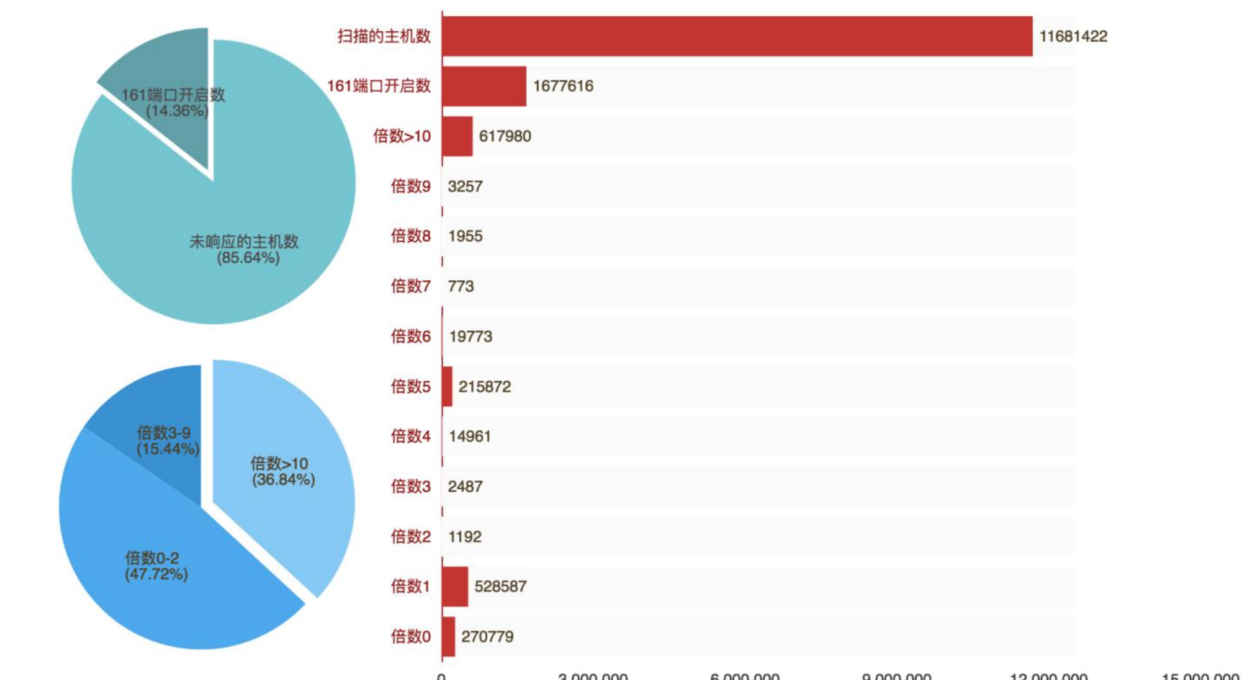
数据来源：ZoomEye网络空间探测引擎

3.3-3 Distribution map of DNS protocol port 53 available hosts in China

3.4. **SNMP**

Through the data obtained by the ZoomEye cyberspace detection engine, there are 11,681,422 hosts that related to the UDP port 161. Then perform magnification detection of these hosts, in fact, only 1,677,616 hosts opened port 161, accounting for 14.36% of the total number. Among the hosts with port 161 open, there are 617,980 hosts with a magnification of more than 10 times, accounting for 36.84% of the total. The specific data is as follows:

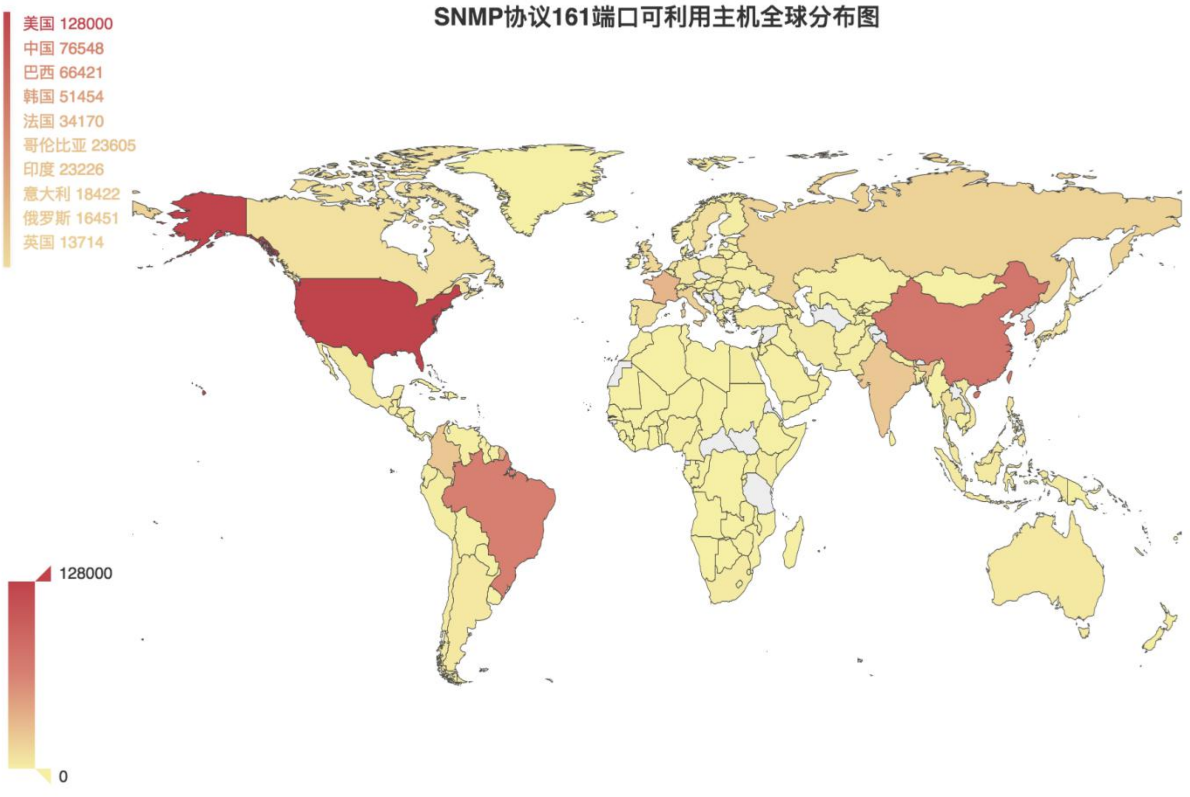
3.4-1 SNMP协议161端口探测统计图



数据来源：ZoomEye网络空间探测引擎

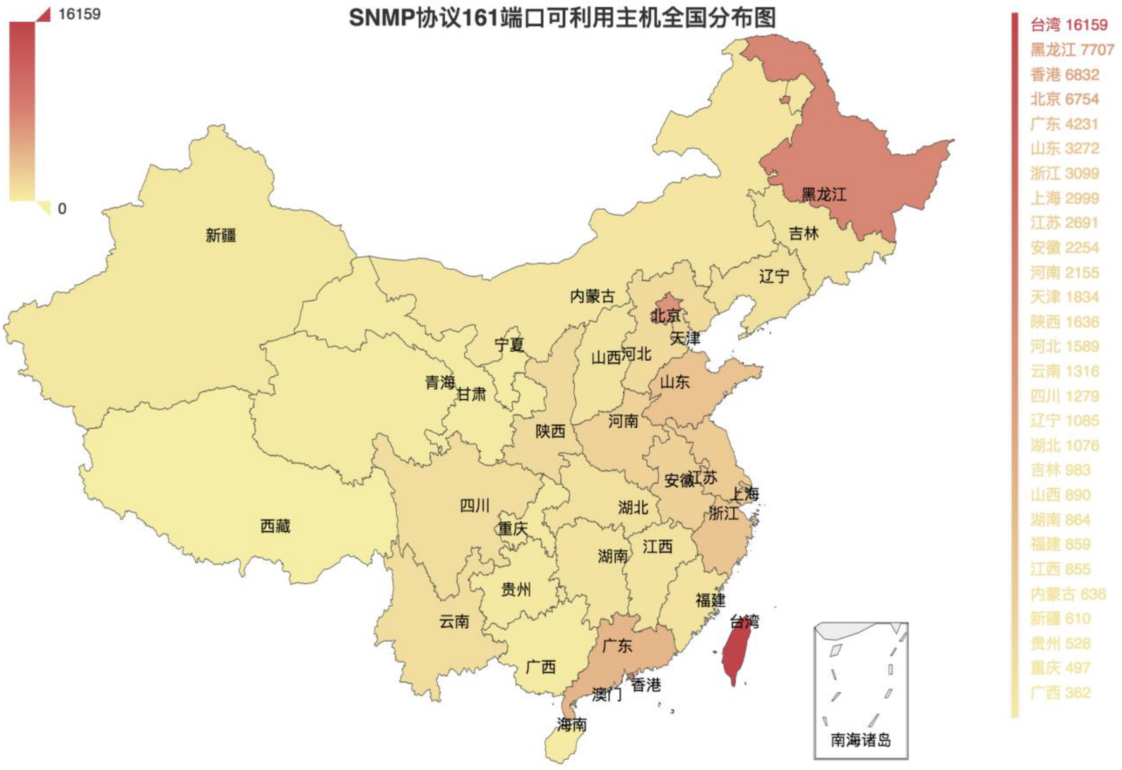
Compared with the previous rounds of data, the number of detected SNMP hosts increased, while the number of available hosts decreased.

Let's take a look at the global distribution of these hosts with a magnification more than 10 times, as shown in Figure 3.4-2. It can be seen that the number of hosts in China has risen to the second place. We also counted the distribution of available hosts in China, as shown in Figure 3.4-3. Taiwan, Beijing, and Heilongjiang are still among the most affected provinces.



数据来源：ZoomEye网络空间探测引擎

3.4-2 Global distribution map of SNMP protocol port 161 available hosts



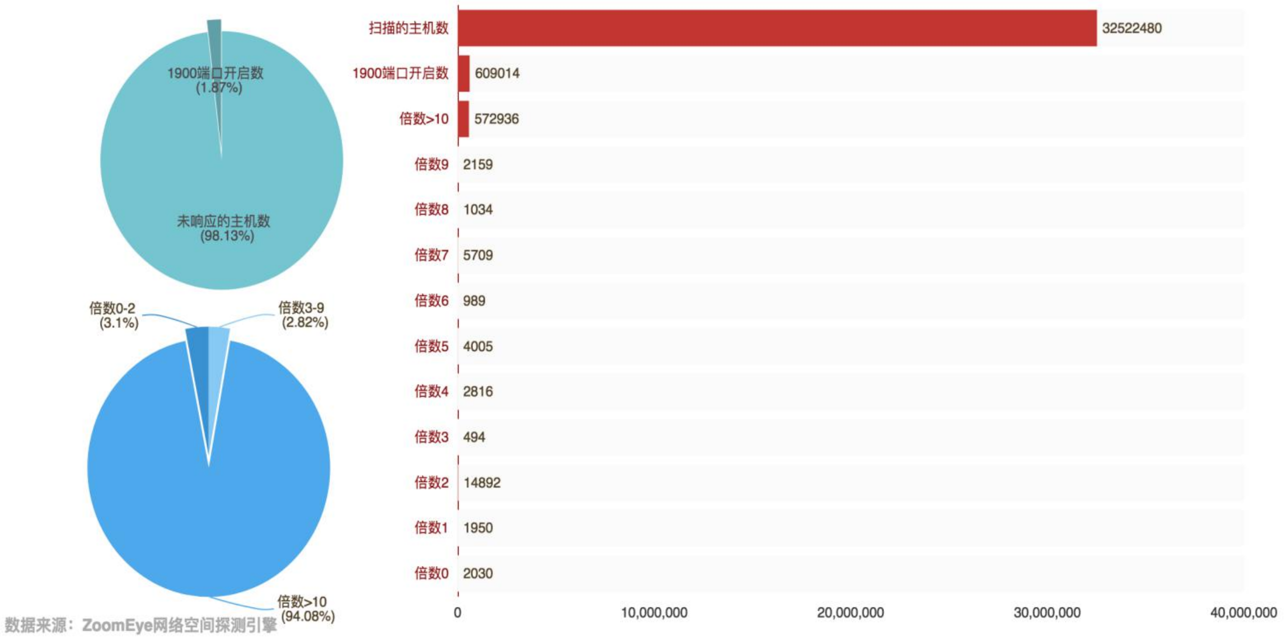
数据来源：ZoomEye网络空间探测引擎

3.4-3 Distribution map of SNMP protocol port 161 available hosts in China

3.5. SSDP

Through the data obtained by the ZoomEye cyberspace detection engine, there are 32,522,480 hosts that related to the UDP port 1900. Then perform magnification detection of these hosts, in fact, only 609,014 hosts opened port 1900, accounting for 1.87% of the total number. Among the hosts with port 1900 open, there are 572,936 hosts with a magnification of more than 10 times, accounting for 94.08% of the total. The specific data is as follows:

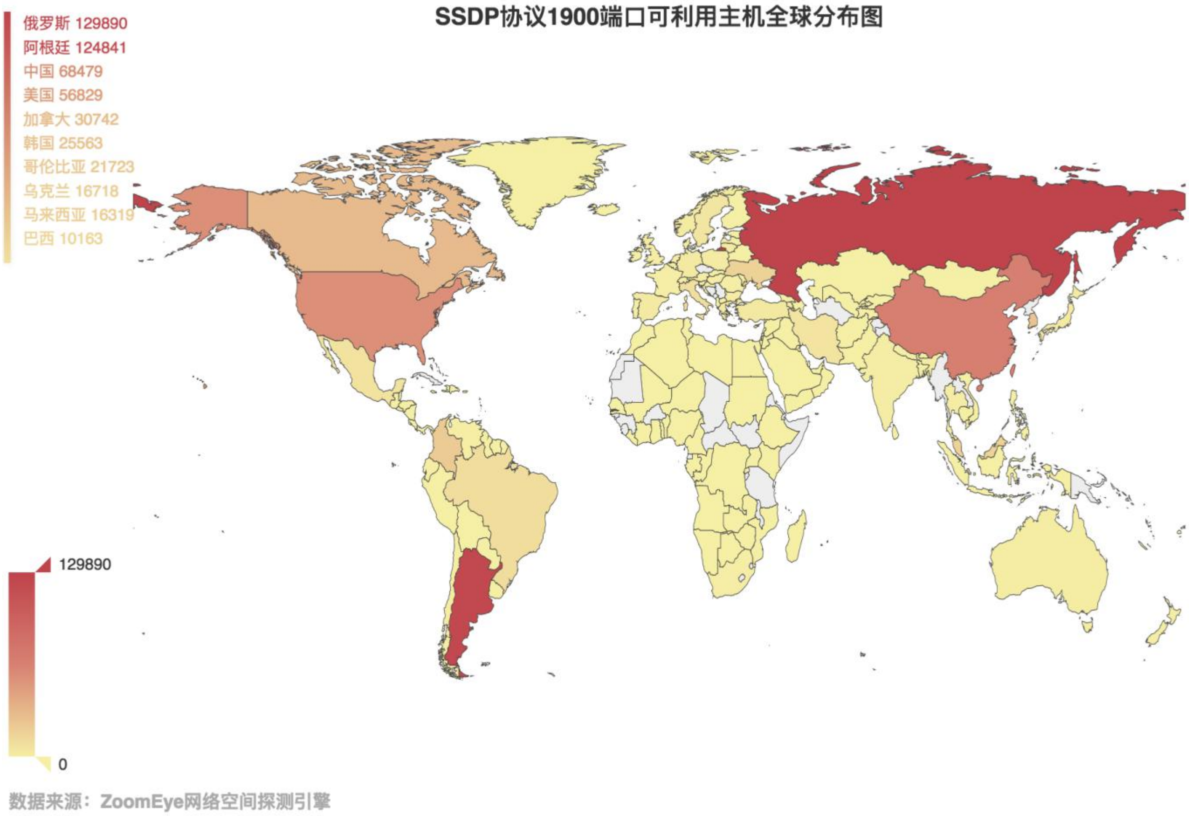
3.5-1 SSDP协议1900端口探测统计图



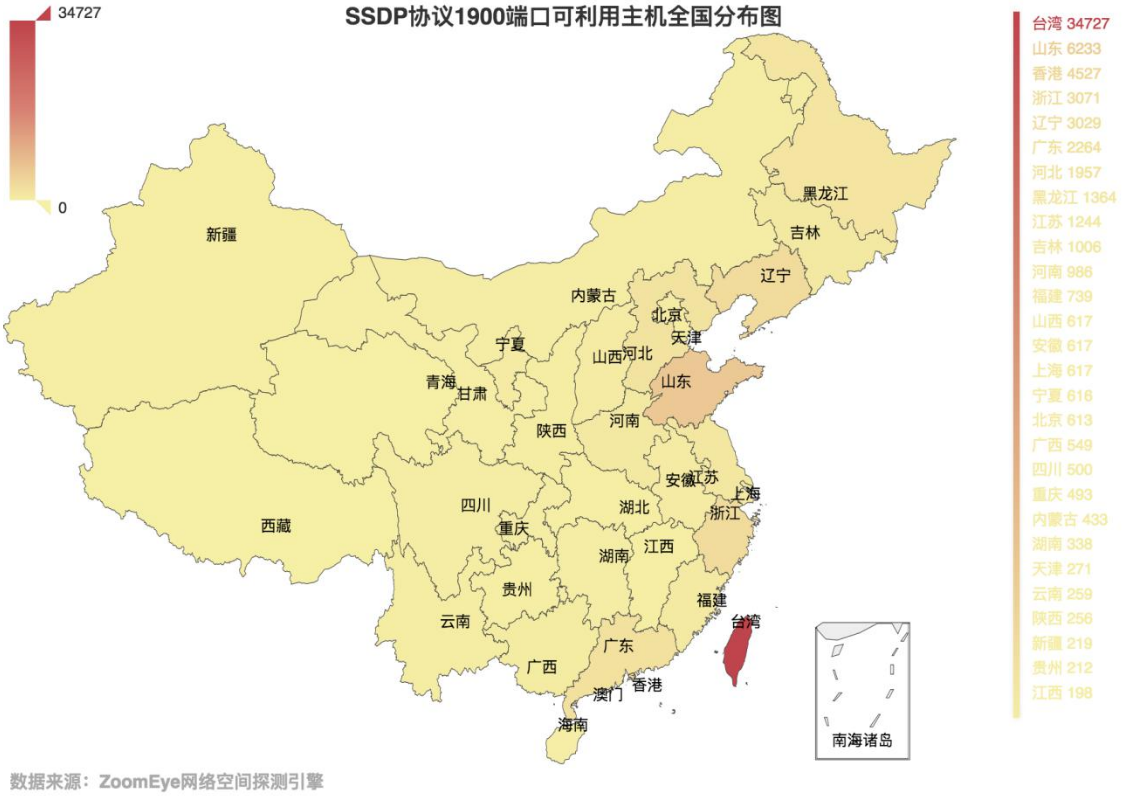
数据来源：ZoomEye网络空间探测引擎

Through the data obtained by the Zoomeye cyberspace detection engine, there are 475,643 hosts related to the UDP port 5683. Then perform magnification detection of these hosts, in fact, there are 192,495 hosts opened port 5683, accounting for 40.47% of the total number. Among the hosts with port 5683 open, there are 56,940 hosts with a magnification of more than 10 times, accounting for 29.58% of the total. The specific data is as follows:, as shown in Figure 3.5-2. There is no significant change from the previous rounds of data.

Statistics on China's data, as shown in Figure 3.5-3, Taiwan is still the province with the largest number of hosts available in China, far exceeding other provinces.



3.5-2 Global distribution map of SSDP protocol port 1900 available hosts

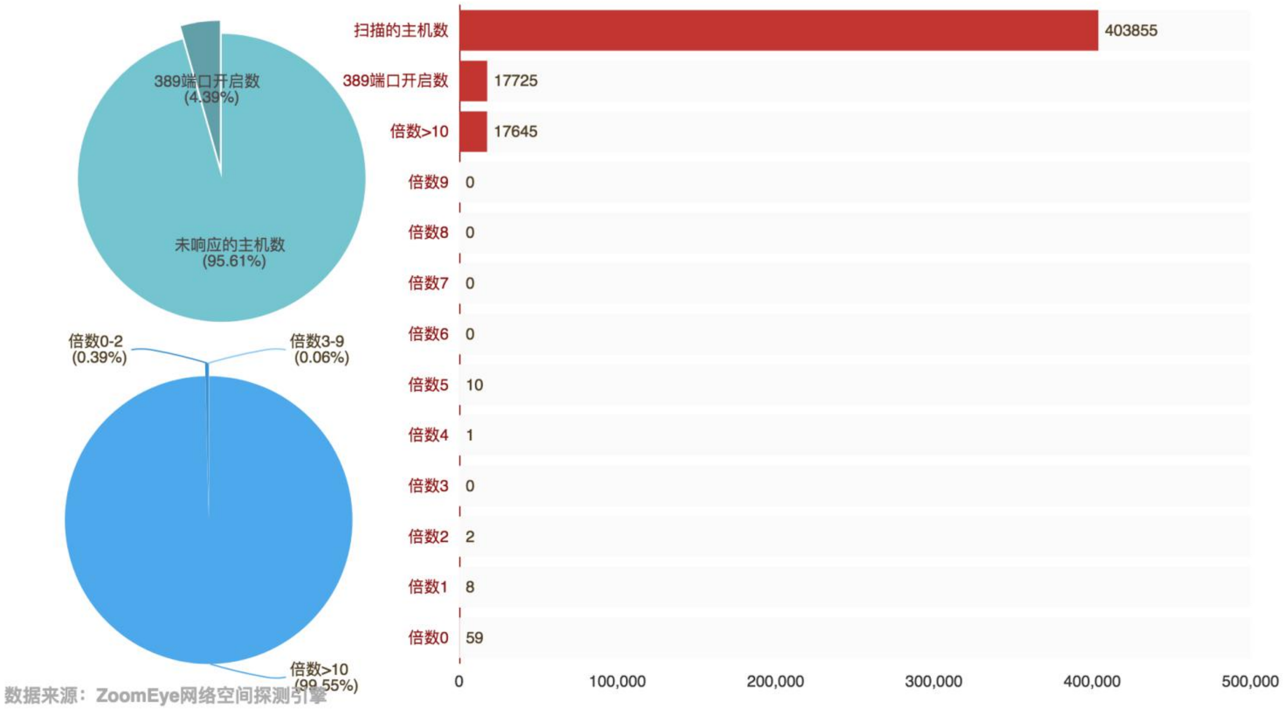


3.5-3 Distribution map of SSDP protocol port 1900 available hosts in China

3.6. **CLDAP**

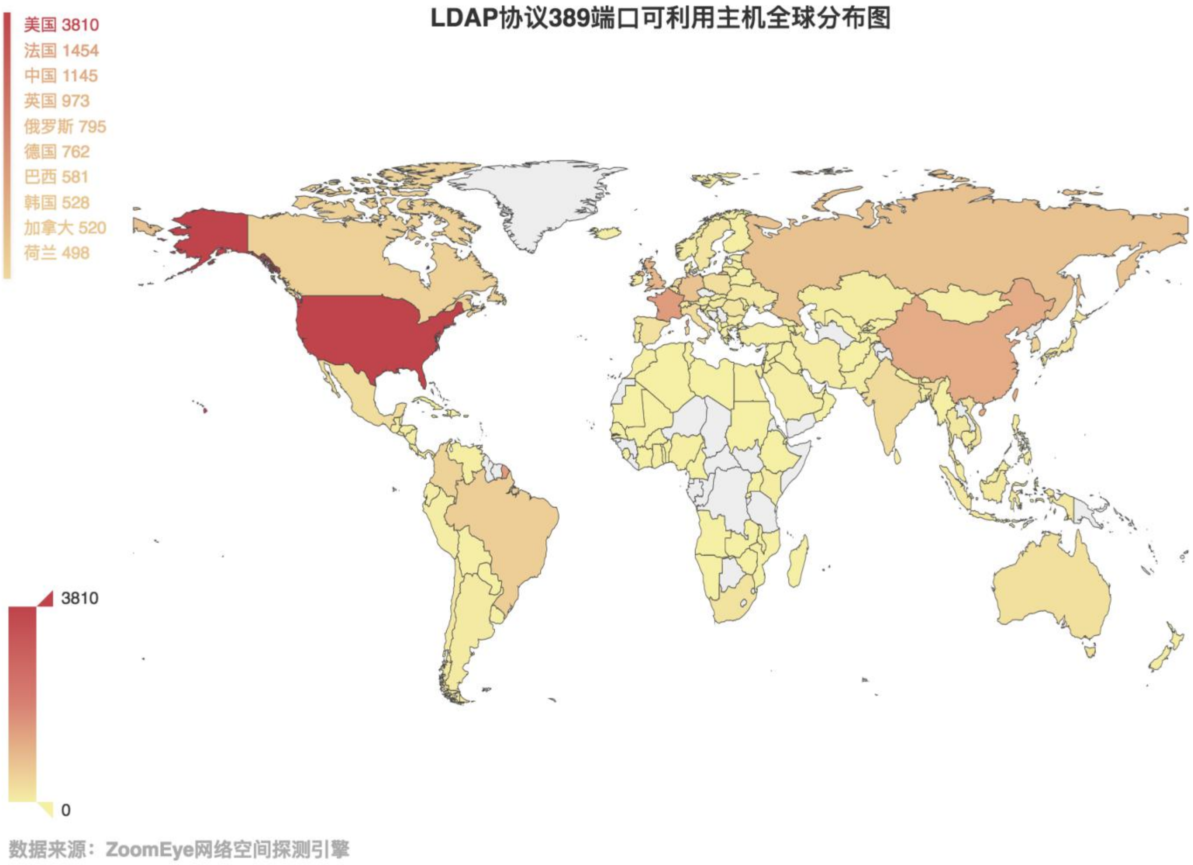
Through the data obtained by the ZoomEye cyberspace detection engine, there are 403,855 hosts that related to the UDP port 389. Then perform magnification detection of these hosts, in fact, only 17,725 hosts opened port 389, accounting for 4.39% of the total number. Among the hosts with port 389 open, there are 17,645 hosts with a magnification of more than 10 times, accounting for 99.55% of the total. The specific data is as follows:

3.6-1 LDAP协议389端口探测统计图



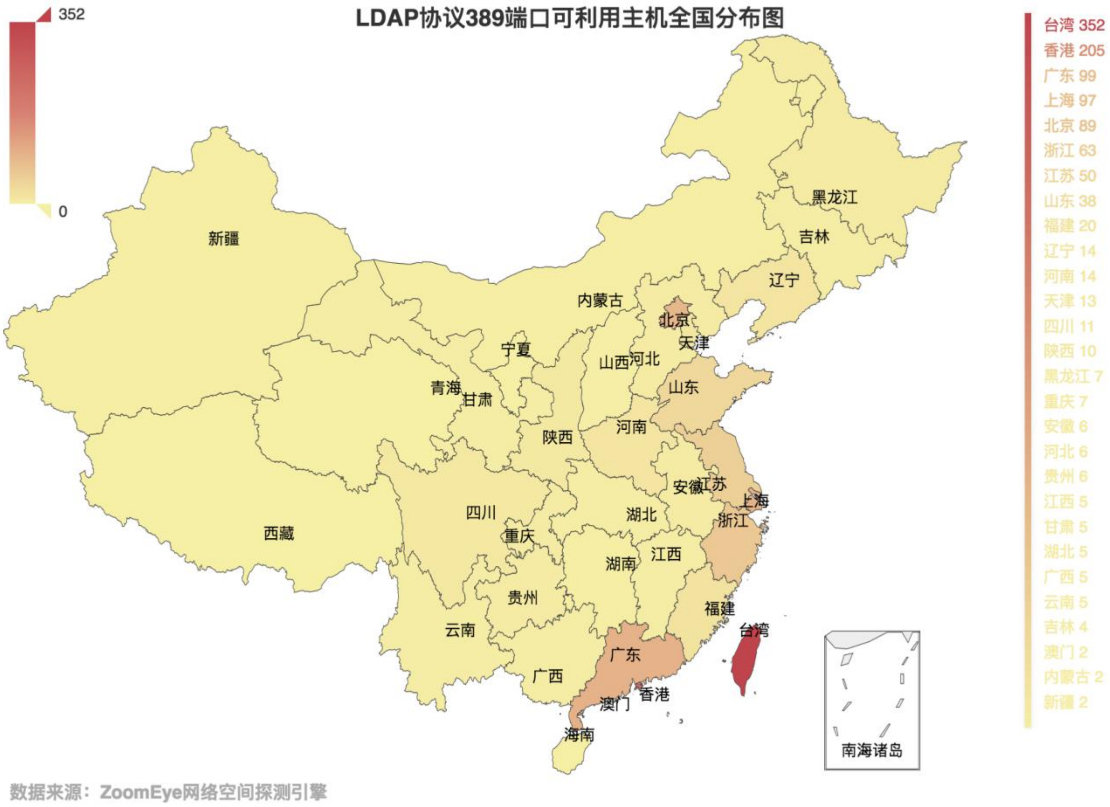
数据来源：ZoomEye网络空间探测引擎

Then take a look at the global distribution of these hosts with a magnification more than 10 times. As shown in Figure 3.5-2, we can see that the United States is still the country with the largest number of CLDAP servers available, and China is still ranked third. We have also made statistics on the distribution of available hosts in China, as shown in Figure 3.5-3, Taiwan is still the province with the largest number of hosts available in China, and Hong Kong is also far more than other provinces in China.



数据来源：ZoomEye网络空间探测引擎

3.6-2 Global distribution map of LDAP protocol port 389 available hosts



数据来源：ZoomEye网络空间探测引擎

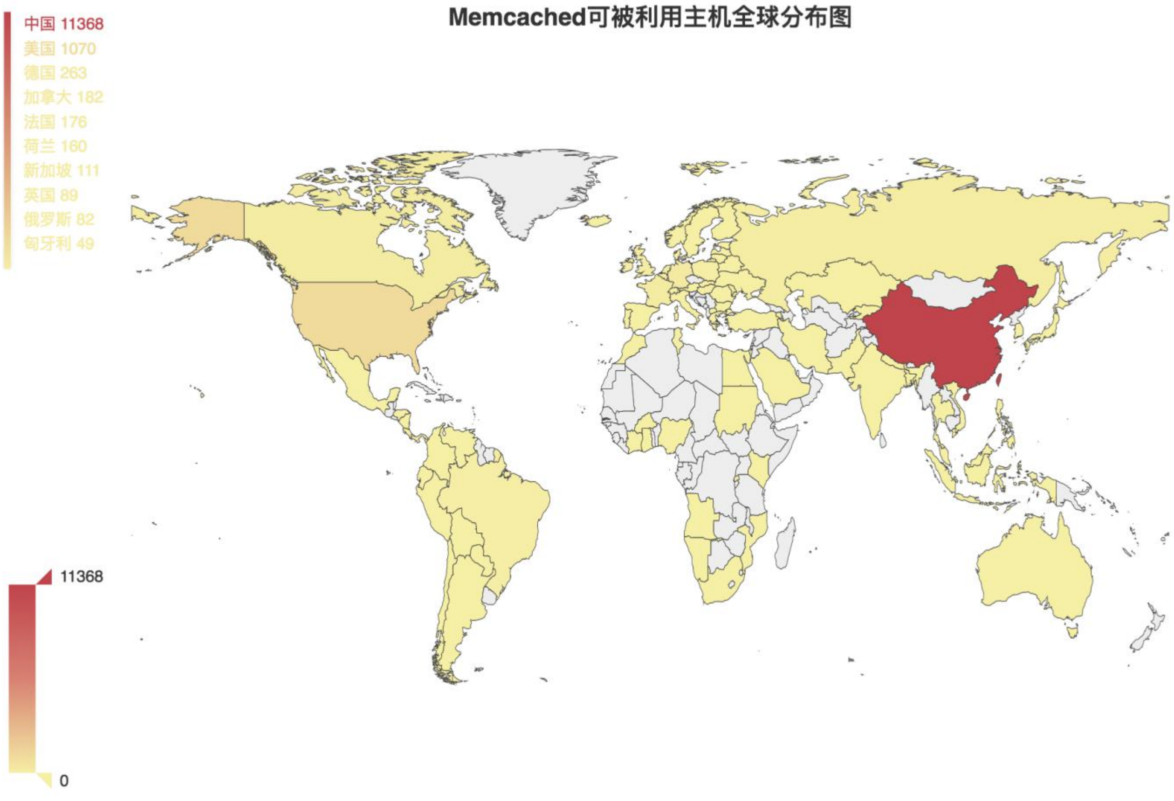
3.6-3 Distribution map of LDAP protocol port 389 available hosts in China

3.7. Memcached

Memcached is a free, open source, high performance, distributed memory object caching system. It is a software developed by Brad Fitzpatric of LiveJournal's Danga Interactive. Now it has become an important factor in improving the scalability of Web applications among many services such as mixi, hatena, Facebook, Vox, and LiveJournal.

Memcached is a memory-based key-value store used to store small pieces of arbitrary data (strings, objects). This data can be the result of a database call, an API call, or a page render. Memcached is simple and powerful, its compact design facilitates rapid development, eases development, and solves many problems with large data caches. Its API is compatible with most popular development languages. Essentially, it's a simple key-value storage system. The general purpose of the application is to reduce the number of database accesses by caching database query results, thereby increasing the speed and scalability of dynamic web applications.

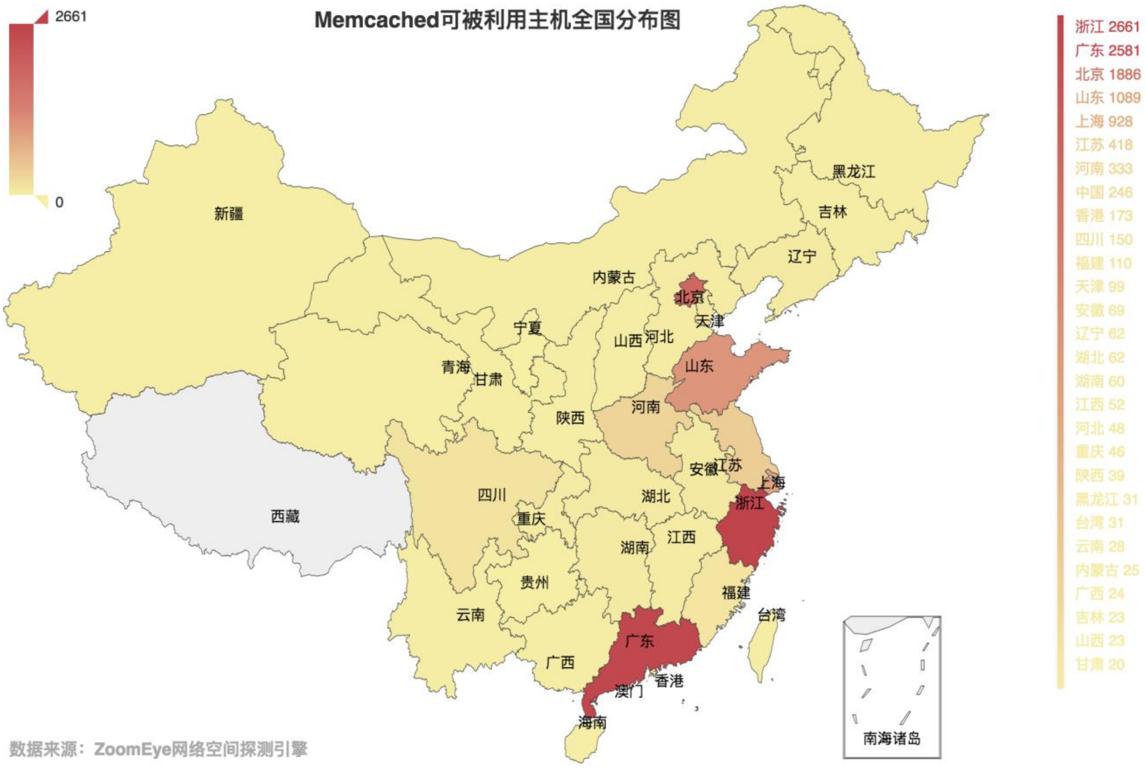
Memcached Server opens TCP/UDP port 11211 by default and uses Memcached's storage service without authentication. On March 2nd, 2018, ZoomEye detected Memcached on the whole network that opened UDP port 11211 and didn't need to authenticate. A total of 14,142 targets were obtained, and global distribution statistics are as shown in Figure 3.7-1:



数据来源：ZoomEye网络空间探测引擎

3.7-1 Global distribution map of Memcached available hosts

Clearly, China’s emphasis on security issues still has a large gap with other countries. Among the 14142 effective targets, 11368 targets IP addresses located in China. The distribution of China's targets are as shown in Figure 3.7-2:

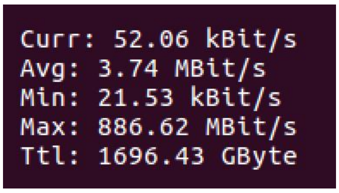


3.7-2 Distribution map of Memcached available hosts in China

When authentication is not turned on, anyone can access the Memcached server, store key-value pairs, and then get the value by key. Therefore, we can store a 1 byte data with a value of 1 kb in Memcached, and then we get the value through the key, which produces nearly 1000 times the magnification effect. Memcached also turns on UDP port by default, so this allows Memcached to be exploited for amplified reflection DDoS attack. The times Memcached can be magnified depends on:

1. Memcached server bandwidth
2. The maximum length of the value that Memcached can store

Test with our own server, first let Memcached store a value of 1kb length, and then get the value to all targets at the same time, it can receive 886Mbit/s of traffic, as shown in Figure 3.7-3:



```
Curr: 52.06 kBit/s
Avg: 3.74 MBit/s
Min: 21.53 kBit/s
Max: 886.62 MBit/s
Ttl: 1696.43 GByte
```

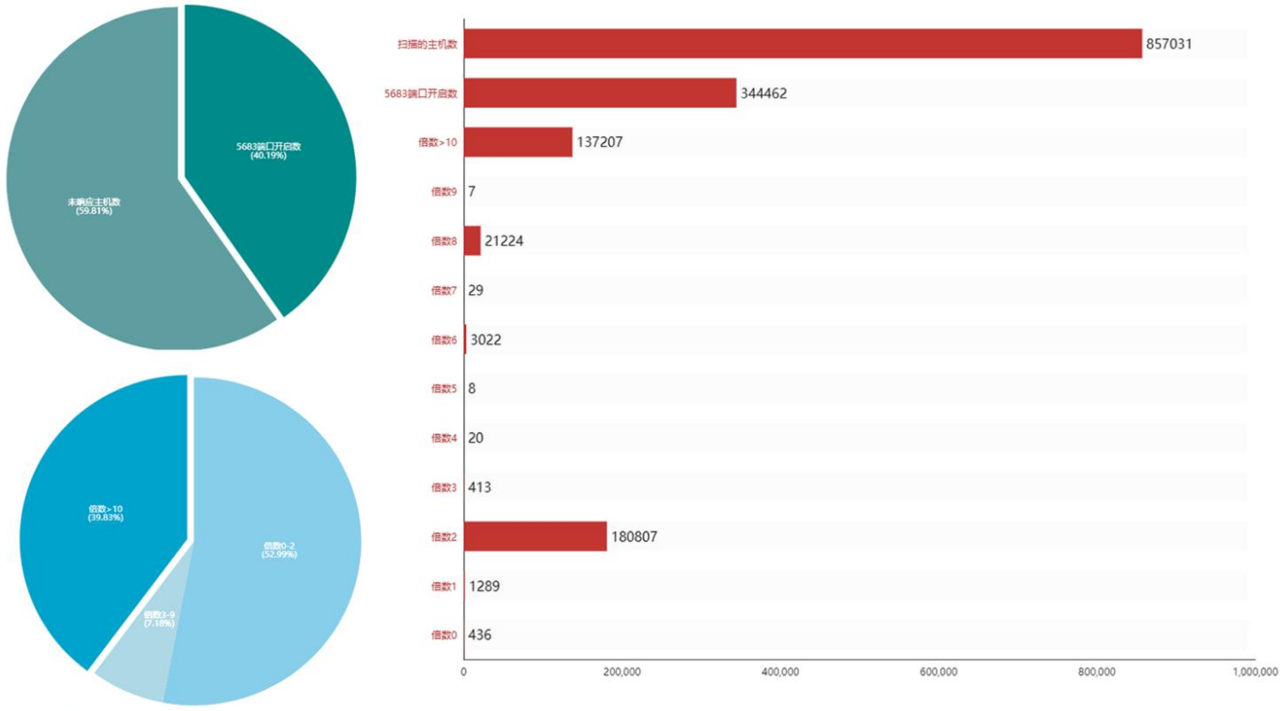
3.7-3 Traffic statistics

3.8. CoAP

CoAP (Constrained Application Protocol) is an application layer protocol applied in the Internet of Things, the detailed definition of whom is in RFC 7252. For most IoT devices, they are primarily resource-constrained devices such as limited CPU, RAM, bandwidth, and so on, so it is extravagant to use the existing network's TCP and HTTP to implement communication between devices. In order to allow these limited resource devices to get access to the network smoothly, the CoAP protocol comes into being. CoAP refers to a restricted application protocol, which is just like the HTTP protocol based on UDP. Compared with HTTP protocol, CoAP inherits its characteristics of reliable transmission, data retransmission, block retransmission, IP multicast and so on. What's more, CoAP uses binary format to pass data, which makes CoAP requests more lightweight and takes up less bandwidth.

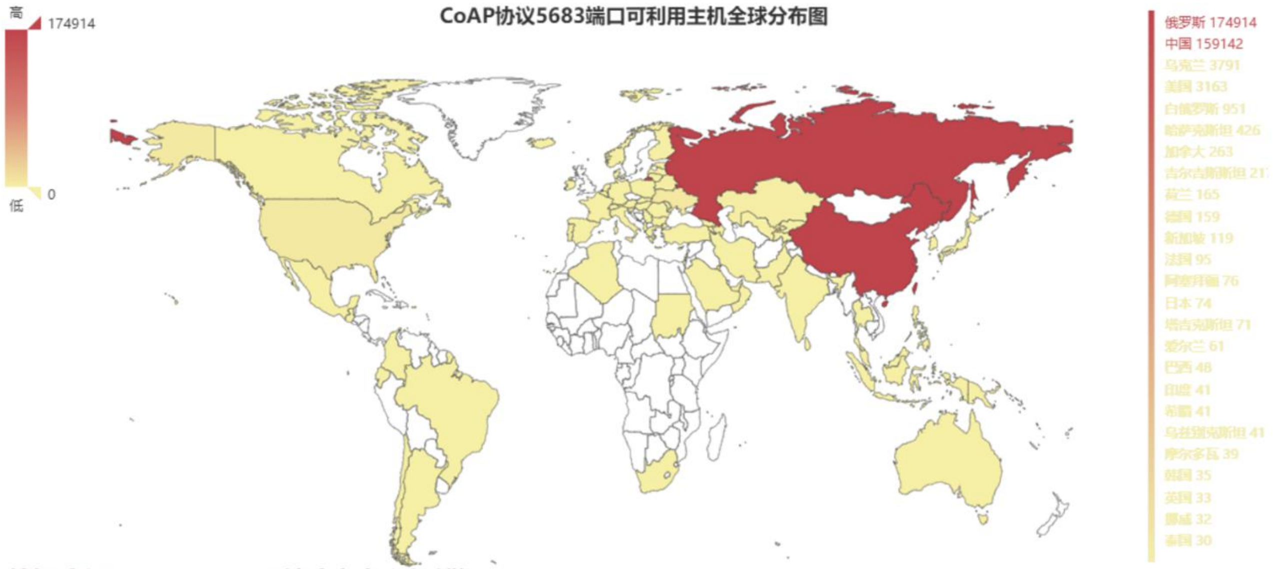
The CoAP protocol specifies that the service device must provide Uri-path of ./well-known/core and be bound to the port 5683 by default. On May 6th, 2019, through the data obtained by the Zoomeye cyberspace detection engine, there were 857,031 hosts related to the UDP port 5683. After performing the magnification detection of these hosts, in fact, there were 344,462 hosts that opened port 5683, accounting for 40.19% of the total number. Among the hosts opening port 5683, there were 137,207 hosts whose magnification was more than 10 times, accounting for 39.83% of the total. The specific data is as follows:

3.8-1 CoAP协议5683端口探测统计图



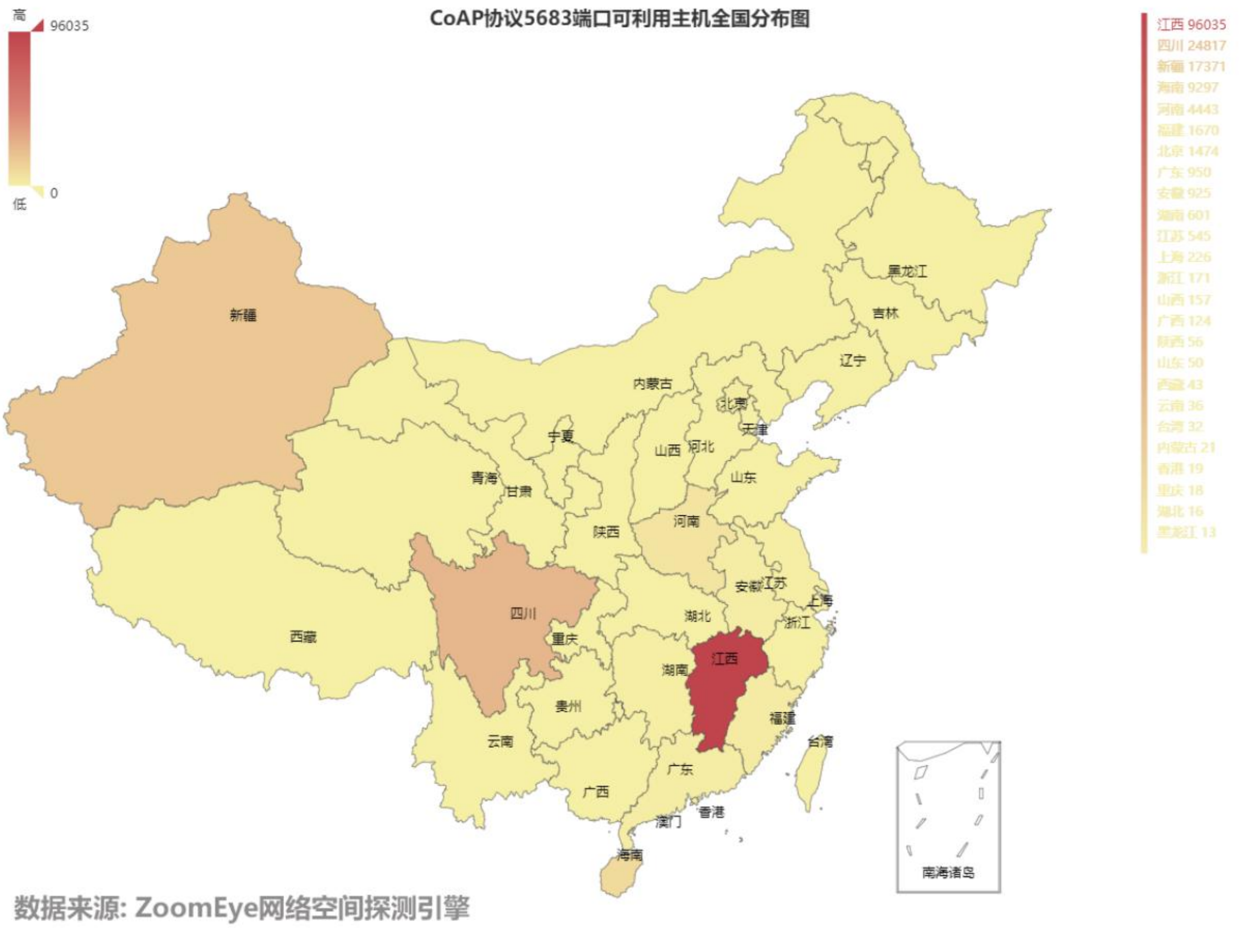
数据来源: ZoomEye网络空间探测引擎

As is shown in Figure 3.8-2, it can be seen that the main distribution of these hosts is in Russia and China. After counting on the distribution of available hosts in China, as is shown in Figure 3.8-3, it can be seen that it's mainly in Jiangxi, Sichuan, and Xinjiang Province. In addition, having conducted a simple analysis of the response packets of Chinese devices, it's found out that a large number of devices contain the keyword--Qlink.



数据来源: ZoomEye网络空间探测引擎

3.8-2 Global distribution map of CoAP protocol port 5683 available hosts



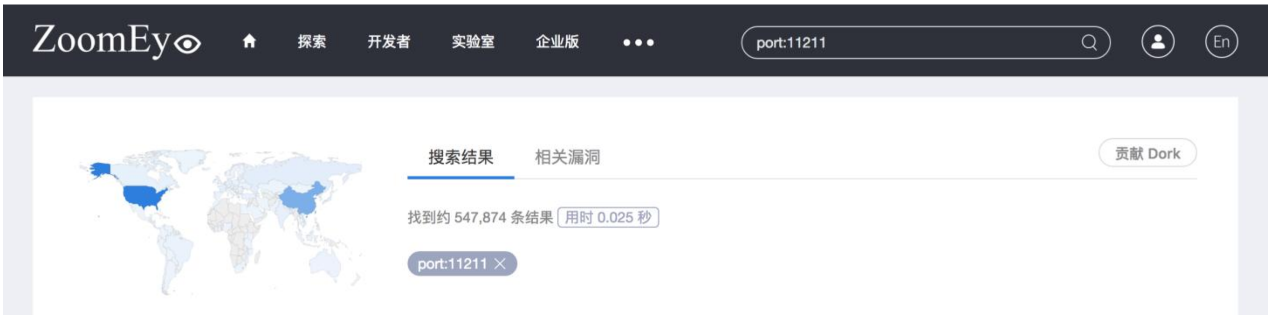
数据来源: ZoomEye网络空间探测引擎

3.8-3 Distribution map of CoAP protocol port 5683 available hosts in China

4. Summary

Compared with the data of the previous three rounds of detection, the biggest change is the NTP service in the fourth round of detection. The current Internet NTP server has been unable to cause large-traffic amplified reflection DDoS attack. In contrast, other protocols have more or less reduced the number of hosts that can be utilized. Amplified reflection DDoS attacks are still very harmful, and DDoS defense is still urgent.

Let’s compare the data detected by ZoomEye with the Memcached service on public network:



找到约 547,874 条结果 用时 0.025 秒

4-4 Number of port 11211 detected by ZoomEye

In ZoomEye's database, there are 540,000 targets for port 11211, including 230,000 in the U.S., and 130,000 in China, but the total number of UDP port 11211 is only 14,142, among which there are 1,070 in the U.S. and 11,368 in China.

From the comparisons of these data, it can be seen that the United States has a very fast response to such security incidents, and the gap between China and the United States is still very large.

From the perspective of magnification, although the available target has been reduced to 10,000, it can still cause a high-traffic DDos attack.

For users of Memcached, we recommend shutting down their UDP port and enabling SASL authentication. For operators, it is recommended to add URPF(Unicast Reverse Path Forwarding) mechanism to the routers, which is a unicast reverse routing lookup technology, used to prevent network attacks based on source address spoofing. By means of this mechanism, it can make UDP reflection attack fail.

As for CoAP, it can be seen from the data collected and analyzed above that the hosts that can be used for DDoS reflection amplification are mainly distributed in Russia and China, and there are many hosts with amplification effects of more than 10 times. For Internet services that use CoAP, you can disable UDP. When you can't disable it, make sure that the request and response do not have a multiple relationship. You can also enable authorization authentication. For enterprise users without UDP related services, you can filter out UDP packets in the upper layer or the local firewall. You can seek operators to provide the IP network segment of UDP black hole to provide external website service. You can also choose to access the DDoS cloud security service or delete the default path of the protocol. For users of Internet of Things, if there is no public network access requirement, the public Network IP should not be enabled; if there is public network access demand, you should add firewall rules, restrict access to IP, and reduce the exposure of devices to the Internet.

5. Reference

1. Stupidly Simple DDoS Protocol (SSDP) generates 100 Gbps DDoS.

   https://blog.cloudflare.com/ssdp-100gbps/

2. The theory and implementation of reflection attack based on snmp

   http://drops.xmd5.com/static/drops/tips-2106.html

3. Research on DRDoS denial of service attack technology based on Memcached distributed system.

   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

6. About Knownsec & 404 Team

Beijing Knownsec Information Technology Co., Ltd. was established by a group of high-profile international security experts. It has over a hundred frontier security talents nationwide as the core security research team to provide long-term internationally advanced network security solutions for the government and enterprises.

Knownsec's specialties include network attack and defense integrated technologies and product R&D under new situations. It provides visualization solutions that meet the world-class security technology standards and enhances the security monitoring, alarm and defense abilities of customer networks with its industry-leading capabilities in cloud computing and big data processing. The company's technical strength is strongly recognized by the State Ministry of Public Security, the Central Government Procurement Center, the Ministry of Industry and Information Technology (MIIT), China National Vulnerability Database of Information Security (CNNVD), the Central Bank, the Hong Kong Jockey Club, Microsoft, Zhejiang Satellite TV and other well-known clients.

404 Team, the core security team of Knowsec, is dedicated to the research of security vulnerability and offensive and defensive technology in the fields of Web, IoT, industrial control, blockchain, etc. 404 team has submitted vulnerability research to many well-known vendors such as Microsoft, Apple, Adobe, Tencent, Alibaba, Baidu, etc. And has received a high reputation in the industry.

The most well-known sharing of Knownsec 404 Team includes:KCon Hacking Conference, Seebug Vulnerability Database and ZoomEye Cyberspace Search Engine.