DNSMon

Look at NTP pool using DNS data

Zhang Zaifeng

May 26, 2020 • 8 min read

With the rapid development of the Internet, more and more people have realized the importance of network infrastructure. We don't hear people talk about NTP (**N**etwork **T**ime **P**rotocol) much though.

Whether NTP can work well will affect the operation of most time-based computer system. For example, IPSEC tunnel establishment, TLS certificate validity verification, personal password expiration, crontab task execution, DNSSEC expiration etc. [1].

The NTP protocol is similar to DNS and is one of the oldest protocols on the Internet. Its main function is to keep the time of the device synchronized as its name suggests. The operating systems we use, such as windows, Android or MacOS, are all equipped with their own NTP time server to synchronize the time on the device regularly.

What is NTP pool?

NTP pool project started in Jan 2003, the basic principle is that the domain name "pool.ntp.org" is divided into multiple sub-domains based on specific rules and DNS polling is used on these sub-domains to provide the required server IP address for the client to use.
This technique is actually somewhat similar to the fastflux technology of DNS used by some malwares. For someone who does research on DNS fastflux detection, the

pool.ntp.org is certainly no stranger.
For more information about NTP pool, please refer here [2].

DNSMon

DNSMon is a security system developed by 360netlab based on massive DNS data (about 5% of China DNS traffic) and combined with multi-dimensional data such as whois, web, sandbox, honeypot, etc. to conduct comprehensive analysis, extraction and interception of malicious domain names. Thousands of malicious and highly suspicious domain name blacklists can be generated every day, serving about 20 million users, and have been running steadily for 2.5 years. Under the premise of no rules, more than ten kinds of botnets such as MSRAMiner, GodLua, etc. have been intercepted for mining and DDoS purposes.

Look at NTP pool using DNS data

The use of a small number of domain names in the NTP pool is very common in our DNSMon system due to the huge amount of access requests, as well as a small number of dns names mapping to a large number of scattered IP addresses.

From the DNS perspective, in addition to being able to assess the scale of the NTP pool itself, it can also be used to measure some basic Internet services. After all, almost all networked devices must be time-synchronized. (We do see a small amount of devices having problem synchronizing time but that is less than 0.02%).

The following analysis is based on the data we gathered from 20200519 18:00 CST to 20200520 18:00 CST 24-hour NTP pool data from our DNSMon.

Number of service users

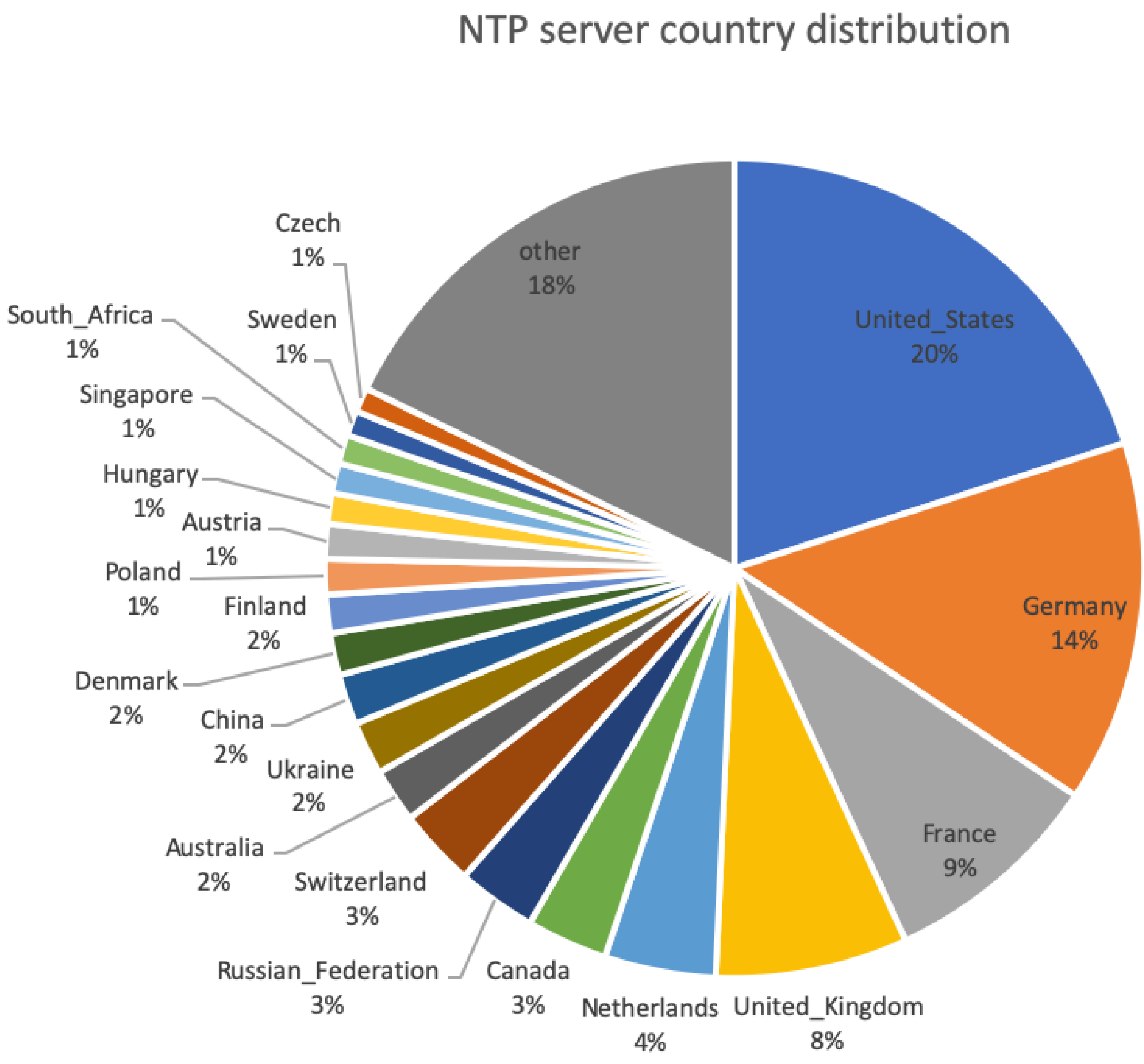
On it’s official NTP pool website, it shows that the number of its users is between 5 million and 15 million [3], and the server IP is around 4000 [4].
During the 24-hour period, a total of 880,000 different clients accessed the time

synchronization service provided by the NTP pool. Considering the data coverage of our system, the number of users who use the NTP pool time synchronization service in China is quite near the upper limit of the number of users declared on their official website.

servers

Basic statistics

The number of NTP pool server IPs is 3758, including IPv6: 1028 and IPv4: 2730, distributed in 97 countries and regions around the world. It is mainly concentrated in countries with good developed networks such as the United States, Germany, France, Britain, Netherlands, and Canada. The specific distribution map is as follows:



NTP server in China

As can be seen from the above figure, the number of domestic NTP server IP accounts for only 2% of the total number of active IPs in the total NTP pool. This value is much lower than the proportion of other network services.
There are 25 domestic operators in the NTP pool, the break downs is:

```
      7 3462|Data_Communication_Business_Group
      6 37963|Hangzhou_Alibaba_Advertising_Co.,Ltd.
      5 4538|China_Education_and_Research_Network_Center
      5 45090|Shenzhen_Tencent_Computer_Systems_Company_Limited
      4 132203|Tencent_Building,_Kejizhongyi_Avenue
      3 4808|China_Unicom_Beijing_Province_Network
      2 9381|HKBN_Enterprise_Solutions_HK_Limited
      2 9304|HGC_Global_Communications_Limited
      2 36351|SoftLayer_Technologies_Inc.
      2 133752|Leaseweb_Asia_Pacific_pte._ltd.
      2 10229|Internet_Content_Provider
      1 9312|xTom
      1 8075|Microsoft_Corporation
      1 58461|No.288,Fu-chun_Road
      1 55990|Huawei_Cloud_Service_data_center
      1 5580|Hibernia_Networks_(Netherlands)_BV
      1 4847|China_Networks_Inter-Exchange
      1 4780|Digital_United_Inc.
      1 4609|Companhia_de_Telecomunicacoes_de_Macau_SARL
      1 45102|Alibaba_(US)_Technology_Co.,_Ltd.
      1 4134|No.31,Jin-rong_Street
      1 23734|Netrouting_Inc
      1 17964|Beijing_Dian-Xin-Tong_Network_Technologies_Co.,_Ltd.
      1 139240|Starch_Works
      1 131584|Taiwan_Intelligent_Fiber_Optic_Network_Co.,Ltd.
```

From the geographical point of view, the domestic IP in the NTP pool is mainly concentrated in Hong Kong, Taiwan, Guangdong and Beijing. The specific distribution is as follows:

```
     18 Hong_Kong
     11 Taiwan
      9 Guangdong
      6 Beijing
      4 Liaoning
      2 Shandong
      1 Zhejiang
      1 Sichuan
      1 Macau
      1 Guangxi
```

NTP pool subdomain distribution

At present, the categories of subdomains are mainly divided into three ways:

- By continent
- By country
- By vendor

Among them, the continents and countries are divided based on the concept of geographical zoning. The core idea is similar to the ECS in DNS. Try to provide an NTP server that is close to the geographical location of the user's source.

The NTP pool for vendor provides sub-domain names with a high degree of identification for specific vendors (router vendors, operating systems, and other hardware and software vendors). Vendors can directly use the subdomains provided by NTP pool within their products. Something like this:

```
0.vendor.pool.ntp.org
1.vendor.pool.ntp.org
2.vendor.pool.ntp.org
3.vendor.pool.ntp.org
```

Visit here for the NTP pool for vendor page here to get more details [5].

Some Basic subdomain numbers

According to our statistics, within 24 hours, there are 682 NTP Pool domain names showed up in our DNSMon, including 534 valid subdomains and 148 invalid subdomains (see the next section). The sub-domain names on top of the list are as follows, as expected, mainly based on countries and regions such as: cn/hk/tw/jp/sg and visits based on Asia. The other perspective is based on the access of OS such as android/openwrt/centos, and the access of native [0-3] .pool.ntp.org.

```
  146677 "cn.pool.ntp.org"
  145710 "asia.pool.ntp.org"
```

```
 143637 "2.android.pool.ntp.org"
 109730 "1.cn.pool.ntp.org"
 109123 "hk.pool.ntp.org"
 108859 "tw.pool.ntp.org"
 107648 "jp.pool.ntp.org"
 107471 "sg.pool.ntp.org"
  93682 "2.asia.pool.ntp.org"
  91415 "0.pool.ntp.org"
  82659 "pool.ntp.org"
  81139 "0.cn.pool.ntp.org"
  77800 "0.asia.pool.ntp.org"
  77077 "2.pool.ntp.org"
  73512 "3.cn.pool.ntp.org"
  72855 "1.asia.pool.ntp.org"
  71965 "2.openwrt.pool.ntp.org"
  71907 "3.pool.ntp.org"
  70814 "1.pool.ntp.org"
  70158 "0.centos.pool.ntp.org"
```

Differences in access by different vendors

Among the TOP subdomains, we see vendor names such as android / openwrt / centos. We digged into our data and have generated the following word cloud according to the number of visits:

The vendors include not only the common Linux releases, but also some network equipment manufacturers, as well as some consumer smart devices and security network products. From the security perspective, some users probably don’t really want their devices type to be leaked this way.

Invalid subdomain

We found that nearly 3% of the DNS request domain names of the NTP pool are invalid. There are 148 invalid domain names (except ap.pool.ntp. org, of which NTP time synchronization service was provided but later stopped, none of the remaining domain names have provided NTP time synchronization services).

- Old devices which have not got the necessary update so they still use old NTP pool domain such as the aforementioned domain name:

ap.pool.ntp.org

- The initial built-in NTP pool domain name has typo, such as: asis.pool.ntp.org, asian.pool.ntp.org, etc.
- Buggy NTP client causes the wrong domain name to be requested, for example, the wrong prefix "www" was accidently added, example: www.africa.pool.ntp.org, www.europe.pool.ntp.org, www.oceania.pool.ntp.org etc.

The TOP 50 domain name and the number of requests (accounting for 98.26% of the total number of invalid requests) are as follows:

```
  18468 "2.generic.pool.ntp.org"
  18423 "1.generic.pool.ntp.org"
  18407 "0.generic.pool.ntp.org"
  18374 "3.generic.pool.ntp.org"
   3676 "4.pool.ntp.org"
   1538 "www.2.android.pool.ntp.org"
   1372 "www.africa.pool.ntp.org"
   1360 "www.europe.pool.ntp.org"
   1357 "www.south-america.pool.ntp.org"
   1339 "www.asia.pool.ntp.org"
   1331 "4.asia.pool.ntp.org"
   1318 "www.oceania.pool.ntp.org"
   1306 "www.north-america.pool.ntp.org"
   1285 "ntp.pool.ntp.org"
   1252 "asian.pool.ntp.org"
   1212 "north.pool.ntp.org"
   1163 "south.pool.ntp.org"
   1121 "e.g.pool.ntp.org"
   1014 "0.ol.pool.ntp.org"
   1000 "1.ol.pool.ntp.org"
    997 "3.ol.pool.ntp.org"
    980 "2.ol.pool.ntp.org"
    927 "0.vmware.pool.ntp.org1.vmware.pool.ntp.org"
    893 "www.1.centos.pool.ntp.org"
    891 "www.0.centos.pool.ntp.org"
    856 "www.0.asia.pool.ntp.org"
    639 "sg.cn.pool.ntp.org"
    548 "5.pool.ntp.org"
    445 "cn1.pool.ntp.org"
    411 "asis.pool.ntp.org"
    402 "china.pool.ntp.org"
    362 "-pcn.pool.ntp.org"
    320 "n.pool.ntp.org"
    320 "america.pool.ntp.org"
    215 "2.euleros.pool.ntp.org"
    205 "2.android2.pool.ntp.org"
    198 "0.euleros.pool.ntp.org"
    192 "2.android1.pool.ntp.org"
    190 "3.euleros.pool.ntp.org"
    185 "1.euleros.pool.ntp.org"
    178 "4.cn.pool.ntp.org"
    157 "172.130.192.250.cn.pool.ntp.org"
    136 "norch-america.pool.ntp.org"
    136 "1.librecmc.pool.ntp.org"
    129 "2.librecmc.pool.ntp.org"
    125 "qqqqqqq2.android.pool.ntp.org"
    121 "0.librecmc.pool.ntp.org"
    119 "aisa.pool.ntp.org"
    118 "3.librecmc.pool.ntp.org"
    103 "0.isoft.pool.ntp.org"
```

NTP pool DNS polling efficiency

As mentioned earlier, the NTP pool uses DNS polling based on the pool subdomain to provide the required server IP to the client. Our DNSMon can measure the efficiency of its DNS polling by counting the rrset frequency of A / AAAA records in DNS.

In theory, if the load balancing is good, the chances of different IPs combining into rrset are equal.

However, due to the influence of geographic location, service capabilities of different servers, and service strategies of different servers in actual operation, the number of different IP combinations for rrset vary greatly. We noticed that the rrset composed of different server IPs returned to the user by the NTP pool is very different.

Our data shows that there are 414,252 rrsets in 3758 IPs, of which TOP4000's rrset (1%) accounts for 41.21% of the total number of records. The cumulative distribution graph of different rrsets is as follows:

Conclusion

1. When we have massive amount of DNS data, various services that use DNS can be well evaluated. NTP pool is a typical example.

2. The number of server IPs in the NTP pool is around 4,000, and the number of users far exceeds 15 million.
3. Domestically, there are not many servers participating NTP pool service and the servers are mainly concentrated in Hong Kong and Taiwan. In mainland China it is mainly concentrated in developed provinces and cities such as Guangdong and Beijing.
4. The access to the NTP pool subdomain is generally successful from a geographical point of view. However, in China, there are large load differences between different servers.
5. About 3% of the domain names requested by the NTP pool are invalid, and almost all the invalid domain names have never provied time synchronization service.
6. DNS request data from the vendor-type subdomain of the NTP pool can be a good assessment of the size and business of specific vendors.

Reference materials

1. https://weberblog.net/why-should-i-run-own-ntp-servers/
2. https://zh.wikipedia.org/wiki/NTP_pool
3. https://www.pool.ntp.org/en/vendors.html#pool-capacity
4. https://www.ntppool.org/zone
5. https://www.ntppool.org/en/vendors.html

0 Comments

1 Login ▾

G

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

♡ Share

Best Newest Oldest

Be the first to comment.

Subscribe Privacy Do Not Sell My Data

— 360 Netlab Blog - Network Security Research Lab at 360 —

DNSMon

俄乌危机中的数字证书：吊销、影响、缓解

商业数字证书签发和使用情况简介(删减版)

An assessment of Non-Authorized Domain Name Resolution provided by DNS Resolution Service Provider

Import 2022-11-30 11:16

The Gafgyt variant vbot seen in its 31 campaigns

Overview Gafgyt botnets have a long history of infecting Linux devices to launch DDoS attacks. While dozens of variants have been detected, new variants are constantly emerging with changes in terms of register message, exploits, and attacking methods. On the other hand, their new botnets are usually short lived, with

DNSMon

从DNS角度看NTP pool服务器的使用

随着互联网的快速发展，其已经深入到日常生活中的方方面面，越来越多的业内人员对于网络基础设施的重要性有了非常深入的认识。不过谈到基础设施，通常都会谈及DNS协议，但是还有一个关键的协议NTP（Network Time Protocol）却没有得到应有的重视。 NTP是否能够良好的工作会影响到计算机系统的大部分基于时间判定的逻辑的正确运...

See all 28 posts →

· Jul 6, 2020 · 7 min read

· May 26, 2020 · 12 min read