DNSMon

从DNS角度看NTP pool服务器的使用

Zhang Zaifeng

May 26, 2020 • 12 min read

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行。比如DNSSEC是否过期，IPSEC的隧道建立，TLS证书的有效性校验，个人密码的过期，crontab任务的执行等等[1]。

NTP协议同DNS类似，是互联网最古老的协议之一，主要作用如其名字所说，用来保持设备时间的同步。在我们使用的操作系统比如windows，Android或者Macos都配置有自己的NTP时间服务器来定期同步设备上的时间。

NTP pool 是什么?

由于互联网的发展以及NTP业务的特殊性（时间需要定期同步），少量的NTP服务器的负载越来越大，并且公共一级NTP授时服务器存在被滥用的问题，2003年1月NTP pool项目正式设立。

其基本原理通过域名“pool.ntp.org”基于特定规则划分为多个子域名并在这些子域名上使用DNS轮询来提供所需的服务器IP地址来给客户端使用，这种技术类似于恶意软件所使用的DNS的fastflux技术，不过要早很多。如果读者基于DNS数据做过fastflux的检测，那么对 pool.ntp.org必然不会陌生，它是去噪的主要对象。

关于NTP pool的更多内容请参考这里[2]。

DNSMon

DNSMon是360netlab开发的基于海量DNS数据（国内5%左右的DNS流量）并结合whois，web，沙箱，蜜罐等多维度数据，对恶意域名进行综合分析，提取和拦截的安全系统。每天可以产生上千条恶意和高可疑域名黑名单，服务于国内大约2000万用户，并已稳定运行2年半。在无规则前提下，已拦截MSRAMiner，GodLua等十余种挖矿，DDoS等僵尸网络。

从DNS数据看NTP pool业务

NTP pool的这种利用少量域名使用DNS轮询来提供IP地址的服务由于访问量巨大，并且映射到大量的分散的IP地址，在DNSMon 中是非常显眼的存在。

从DNS角度除了能够对NTP pool自身业务规模的评估之外，还可以对互联网业务做到大致的评估，毕竟几乎所有的联网设备都要进行时间同步（从DNSMon的数据来看确实有少量的联网设备存在时间漂移问题，设备数量大概不到总数的万分之二）。

为了准确的评估NTP pool的业务情况，我们从DNSMon中选取了20200519 18:00 ~ 20200520 18:00 24小时NTP pool的数据分别从NTP pool自身业务以及使用该服务的互联网用户角度来进行评估。

服务用户数

NTP pool在其官网显示其服务用户数量在500万~1500万之间[3],服务器IP则在4000左右[4]。我们利用DNSMon对其在国内的业务规模做一个简单的评估。

在所收集数据的24小时期间，共有88万不同的客户端访问了NTP pool所提供的时间同步服务。考虑到我们系统的数据覆盖，在国内使用NTP pool时间同步服务的用户数量就会接近其官网声明的用户数量的上限。

服务器情况

基本统计

NTP pool服务器IP数量3758个，其中IPv6：1028个，IPv4:2730个，分布在全球97个国家和地区。主要集中在美、德、法、英、荷、加等网络比较发达的国家，具体分布图如下：

NTP服务器在国内的情况

从上图可以看出，国内NTP服务器的IP个数只占总NTP pool内活跃IP数量的2%。这一数值比其他网络服务所占比例要低的多。

从运营商角度来看，在NTP pool中的国内的运营商共有25家，具体分布如下：

```
      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.
```

从地理位置看来，在NTP pool中的国内的IP主要集中在香港，台湾，广东和北京。具体分布如下：

```
     18 Hong_Kong
     11 Taiwan
      9 Guangdong
```

```
      6 Beijing
      4 Liaoning
      2 Shandong
      1 Zhejiang
      1 Sichuan
      1 Macau
      1 Guangxi
```

NTP pool的子域名分布

NTP pool的子域名是指在 pool.ntp.org下的子域名。现在子域名的类别主要按照三种方式划分：

- 按照大洲划分
- 按照国家划分
- 按照供应商划分

其中按照大洲和国家都是基于地理分区的理念进行划分的，其核心思想和DNS中的ECS类似，尽量提供与用户来源地理位置接近的NTP服务器。
按供应商划分是NTP pool为特定的供应商（路由器厂商，操作系统，其他软硬件厂商）提供的具有高标识度的子域名。供应商可以在其产品内部直接使用NTP pool为其提供的子域名。形如：

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

具体NTP pool为供应商提供服务的细节请参考这里[5]。

子域名的基本情况

经过统计，在24小时内，DNSMon中共有682个NTP Pool域名的访问，其中有534个有效子域名，148个无效子域名（见下一节内容）。其中头部的子域名如下，和预想的一致，主要是基于国家和地区如：cn/hk/tw/jp/sg和基于大洲asia的访问。另一个角度则是基于android/openwrt/centos等OS的访问，还有就是不带有任何属性的原生 [0-3].pool.ntp.org的访问。

```
 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"
```

不同供应商的访问差异

在TOP的子域名中，我们看到了android/openwrt/centos等供应商的信息，这引起了我们的好奇，我们想知道目前利用NTP pool提供时间服务的供应商都有哪些以及他们对应的访问量又如何。基于这个数据，我们对供应商部分做了整理，按照其访问次数统计之后的词云如下：

供应商中既包含了常见的Linux的发行版本信息，也有做网络相关设备的厂家，还有一些消费类的智能设备以及安全类的网络产品。通过NTP pool的子域名分析，得到的这些信息某种程度上存在一定的信息泄漏，需要NTP pool和各厂家重视来解决它。

无效子域名情况

从这24小时的数据中，我们发现有接近3%的NTP pool的DNS请求域名是无效的，无效域名共有148个（其中曾经提供过NTP时间同步服务但是退出的域名只有ap.pool.ntp.org，其余的域名均无提供过NTP时间同步服务）。这可能也是导致部分互联网设备无法有效进行时间同步的一个原因。

根据已有的数据，目前看到的原因主要是如下三个：

- 联网设备是老设备，系统软件没有更新导致内置的NTP pool域名服务器停止服务之后，没有更新到新的域名上来，如刚才提到的域名：*ap.pool.ntp.org*
- 初始内置的NTP pool域名有typo的情况，比如：*asis.pool.ntp.org,asian.pool.ntp.org* 等。
- NTP客户端在实现同步的时候，存在bug，导致请求了错误的域名，增加了错误的前缀“www”，比如：*www.africa.pool.ntp.org,* *www.europe.pool.ntp.org*，*www.oceania.pool.ntp.org* 等。

其中TOP 50的域名及其请求次数(占总无效请求次数的98.26%)如下：

```
 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轮询的效率

之前提到，NTP pool基于池子域名使用DNS轮询来提供所需的服务器IP给客户端使用。通过DNSMon可以清楚的看到其DNS轮询效率如何，统计DNS中A/AAAA记录的rrset组合频次是一个评估轮询效率的方法。理论上来说，如果负载均衡足够好的话，不同的IP互相组合成rrset的机会是均等的。

不过由于实际操作中受到地理位置，不同服务器的服务能力以及不同服务器的服务策略的影响，不同IP组合为rrset的数量会相差甚远。经过统计我们发现，验证了NTP pool返回给用户的不同的服务器IP组成的rrset差别非常大。

我们的数据显示，在3758个IP存在414252个rrset，其中TOP4000的rrset（1%）占总记录数的41.21%。不同rrset的累积分布图如下：

结论

1. 从DNS角度可以很好的评估基于DNS的各种业务，NTP pool是一个很典型的例子。
2. NTP pool的服务器IP数量在4000台左右，用户数量则远超1500万。

3. 国内在NTP pool服务器贡献较少，并且主要集中在香港和台湾地区，大陆主要集中在广东，北京等发达省市。
4. NTP pool子域名的访问从地理位置来看大体上是成功的。但是由于多种策略的原因，在国内来看，不同服务器之间负载存在较大的差异。
5. 在实际使用中，大约3%的NTP pool请求的域名是无效的，并且几乎所有的无效域名从未有过NTP pool的时间同步服务。
6. 从NTP pool的供应商类型的子域名的DNS请求数据可以很好的对具体供应商的规模和业务进行评估。由此引起的安全问题，需要引起供应商，尤其是面向个人消费者的供应商和NTP pool的重视。

参考资料：

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

— 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

DNSMon

Look at NTP pool using DNS data

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 (Network Time Protocol) much though. Whether NTP can work well will affect the operation of most time-based computer system. For example, IPSEC tunnel...

Import 2022-11-30 11:16

New activity of DoubleGuns Group, control hundreds of thousands of bots via public cloud service

See all 28 posts →

· May 26, 2020 · 8 min read

Overview Recently, our DNS data based threat monitoning system DNSmon flagged a suspicious domain pro.csocools.com. The system estimates the scale of infection may well above hundreds of thousands of users. By analyzing the related samples and C2s, We traced its family back to the ShuangQiang(double gun)...

· May 23, 2020 · 16 min read