登录

【反欺诈专栏】关于IP，这里有你想知道的一切！上篇

同小盾 / 2017-07-13 03:29:00 / 浏览数 4985 技术文章 技术文章 顶(0) 踩(0)

Author:戒小贤@同盾反欺诈研究院

今日，就来跟大家聊聊关于IP地址方方面面的研究，其实可以归到三个问题上：

1、这个IP在哪儿？

2、这个IP是什么？

3、这个IP干了什么？

看似简单的问题，但每个都需要投入巨大深入研究的代价。同盾科技在IP画像研发过程中，我们接触了国内外很多出色的IP地址数据服务商，也经过诸多的测试与调研，最终

关于IP的一些冷知识：

IP地址(本文中特指IPv4地址)，是用于标识网络和主机的一种逻辑标识。依托于强大的TCP/IP协议，使得我们可以凭借一个IP地址，就访问互联网上的所有资源。

IP地址本质上，只是一个32位的无符号整型(unsigned int)，范围从0 ~ 2^32
，总计约43亿个IP地址。为了便于使用，一般使用字符串形式的IP地址，也就是我们平常用到的192.168.0.1这种形式。实际上，就是把整数，每8个二进制位转换成对应的十

比如，192.168.0.1和3232235521是等价的。
1

```
→  ~ ping 3232235521
PING 3232235521 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=252 time=4.350 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=252 time=4.444 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=252 time=4.445 ms
```

1
当今全球，互联网系统共分为四大区域，每一个区域都由一件互联网的本体，通过光缆覆盖信号。这四大区域分别被命名为：格兰芬多，斯莱特林，赫奇帕奇以及拉文克劳..

这是《爱情公寓3》中的一个让人捧腹的桥段。虽然是恶搞，但是有一件事儿说对了，互联网确实是分区域的。

全球共有五个区域互联网注册机构(RIR)，分别是：

美洲互联网号码注册管理机构（American Registry for Internet Numbers，ARIN）；

欧洲IP网络资源协调中心（RIPE Network Coordination Centre，RIPE NCC）；

亚太网络信息中心（Asia-Pacific Network Information Centre，APNIC）；

拉丁美洲及加勒比地区互联网地址注册管理机构（Latin American and Caribbean Internet Address Registry，LACNIC）；

非洲网络信息中心（African Network Information Centre，AfriNIC）。

IP地址的划分，有RIR机构来进行统筹管理。负责亚洲地区IP地址分配的，就是APNIC，总部位于澳大利亚墨尔本。

各大RIR机构都提供了关于IP地址划分的登记信息，即whois记录。可以在各大RIR机构提供的whois查询页面上查看，或者使用whois命令查询：

```
- whois -h whois.apnic.net 153.35.93.31
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html
% Information related to '153.34.0.0 - 153.35.255.255'

inetnum:        153.34.0.0 - 153.35.255.255
netname:        UNICOM-JS
descr:          China Unicom Jiangsu province network
descr:          China Unicom
country:        CN
admin-c:        CH1302-AP
tech-c:         LL58-AP
remarks:        service provider
```

whois信息中，会显示IP地址所属的网段，以及申请使用和维护这个网段的运营商。比如，上面的信息中显示，153.35.93.31隶属于江苏省联通。

某些黑客题材的电影中往往会出现使用whois直接查询得到了一个IP的位置，非常精确地定位到了一幢建筑物里。

这张截图来自于2015年上映的《BlackHat》，满满的槽点，都是导演YY出来的。


```
- whois -h whois.apnic.net 153.35.93.31
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html
% Information related to '153.34.0.0 - 153.35.255.255'

inetnum:        153.34.0.0 - 153.35.255.255
netname:        UNICOM-JS
descr:          China Unicom Jiangsu province network
descr:          China Unicom
country:        CN
admin-c:        CH1302-AP
tech-c:         LL58-AP
remarks:        service provider
```


（导演：怪我咯？）

正餐之前，给大家稍加科普一下，下面我们就要进入主菜了。让我们逐一来解惑文章开篇提到的三个问题。

NO.1 **这个IP在哪儿？**

前面提到IP的whois信息，其中包含了申请使用该IP的运营商信息，并且在网段描述信息中，会包含国籍和省份信息。

但是这样远远不够，风控场景中，我们需要更加精确的结果，需要知道这个IP具体在哪个城市、哪个乡镇，甚至希望能够精确到某一条街道或者小区。

曾有人问：我们的IP地址库是否能够提供这样的结果？可以确定用户在某个网吧、写字楼甚至某个小区？

那上面这样的IP数据库是如何产生的呢？

俗称"人海战术"。您可别不相信，直到今天，依然有众多的网友在为这个IP库提供数据更新，上报IP地址的确切位置。但我们无从考证这个位置信息是否真实准确，如果不能

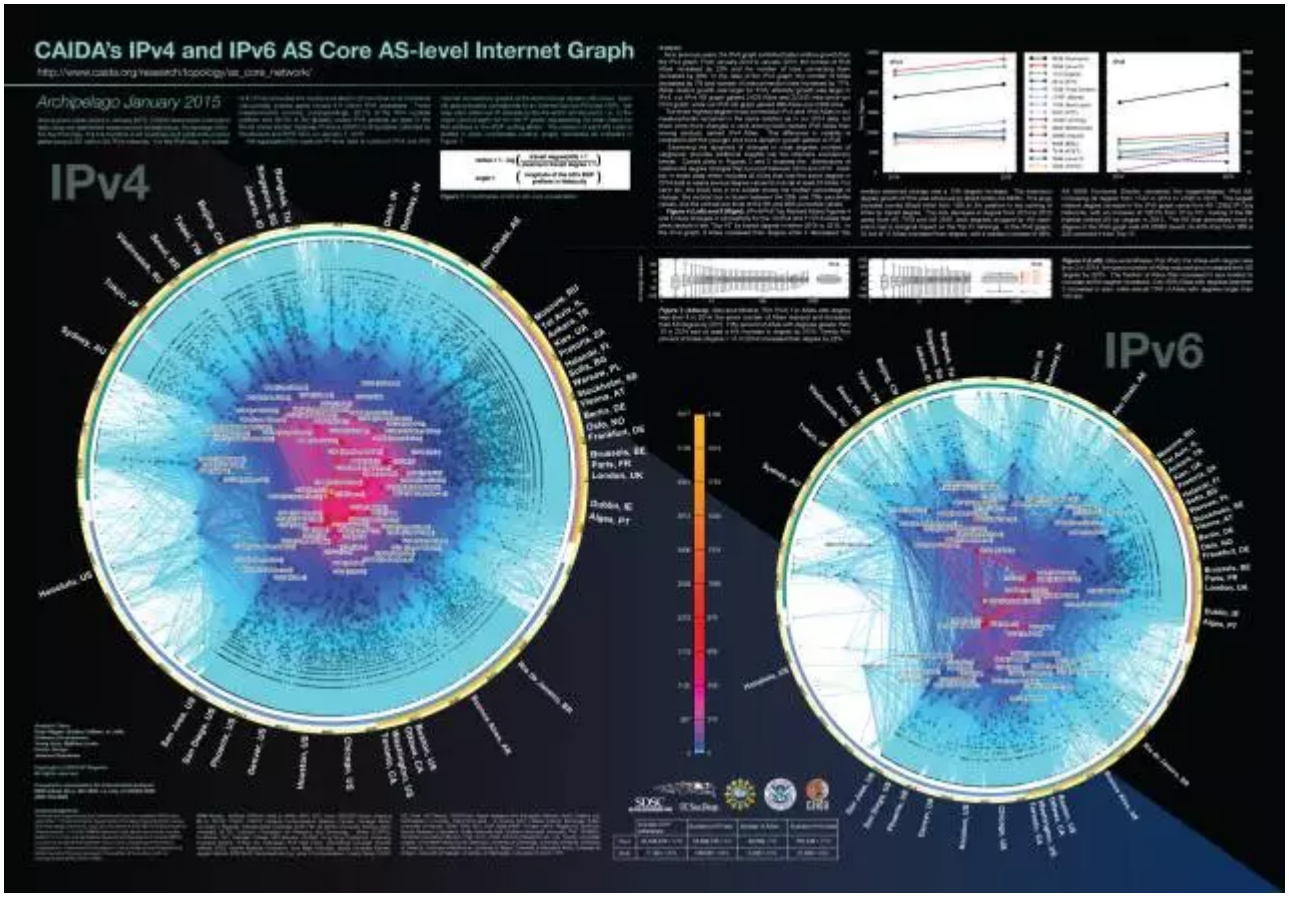
一种IP地址定位手段，是通过海量Traceroute信息来分析。

理论上，如果我能够得到所有IP相互之间Traceroute的信息，就可以绘制出整个互联网的链路图。

(上图来自于IPIP.NET提供的BestTrace工具)

每一次traceroute，都会返回详细的网络链路信息。积累了足够多的链路信息之后，就可以直观地看出，很多链路都经过了同一个IP，那么这个IP就是骨干节点或者区域的骨

以下是CAIDA的一份报告，使用了类似的原理，但统计的最小单位是AS(自治域)



原图地址：[img]http://www.caida.org/research/topology/as_core_network/pics/2015/ascore-2015-jan-ipv4v6-poster-2000x1389.png[/img]圈的边缘，就是探测节

首先，你得有足够数量的节点来探测、收集traceroute链路数据。其次，要有可靠的技术手段来及时分析探测到的结果，汇总形成IP地址数据库。据了解，DigitalElemet也

根据这种网络链路探测的出的定位结果，业内又称之为“网络位置”。就是从互联网的结构上来说，我们最终确定了一个IP，被分配到了某个地方的运营商手里。

但是我们又遇到了很多其他的情况，给大家举几个简单的例子。

117.61.31.0 江苏省 南京市 电信

通过分析这个IP关联的所有定位数据，得到了如下的分布：

这种情况，我们称为“流量回源”。当用户在使用南京电信的手机卡上网时，无论用户身处哪里，他的流量都会回到南京电信，再转发出去，所以从IP上看，都会显示为一个南

上面的定位信息分布，可以在RTB Asia的IP地址实验室中https://ip.rtbasia.com/

153.35.93.32 江苏省 南京市 联通

各种渠道的信息表明，这个IP确实分配到了南京联通，结果定位点全部落在了北京市的范围内。如果我们根据IP的定位结果来判断用户当前的位置，得到的结果肯定就错了。

难道前面提供的信息错了？其实是由于国内运营商对IP地址的划分和使用不透明，甚至特殊形式的租赁，导致北京的用户，分配到了一个南京的IP。

IP地址跨城市覆盖，覆盖范围非常大，用户位置和网络位置不在同一个城市甚至不在同一个省，都会影响到结果，无法准确给出判断。

另一方面，随着移动设备的普及，在用户允许的情况下，可以通过移动设备采集到设备上的GPS信息。前面大家看到的两张定位分布图，就是分析一个IP在历史上关联过的所

这种分析方法看起来效果非常不错，但是却面临两个很重要的问题。

其一是，今年来设备作弊的方式层出不穷，如果没有有效的手段来保证数据的准确性和可靠性，最终得出的结果也会有偏差。

比如下面这里例子，定位点非常规整地分布在一个矩形区域内，而且覆盖到了海面上，做了深入的分析之后才发现这个IP下面有大量的作弊行为：

另一方面，依靠定位点分布来分析IP的定位，需要长时间积累GPS数据。人口密集的地方，这个数据积累可以只要一天，二线城市需要一周，三线城市就需要至少一个月了。

实际的使用中，我们会把这两种方式结合到一起。并不是说，两个定位结果中，有一个错了。两个都是正确答案，只是某些情况下，有一个答案并不适合风控场景。

互联网，就像物流系统一样。我们分析IP的位置，和分析一个快递小哥负责派送的区域原理是一样。没有哪个快递小哥只给一户人家送货，IP也一样，我们最终只能确定这个

□ 本次与大家分享的内容到此为止，大家可以反复多次阅读，很多专业描述其实也没有那么难懂，期望可以帮助到有需要的朋友们。另外两个问题的分享，敬请期待IP下

点击收藏 | 0 关注 | 0

上一篇：【反欺诈专栏】关于IP，这里有你想... 下一篇：【反欺诈专栏】关于IP，这里有你想...

1. 1 条回复

季雨林 2017-07-26 04:56:29

原来我跟楼主在同一个服务商的群里

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板