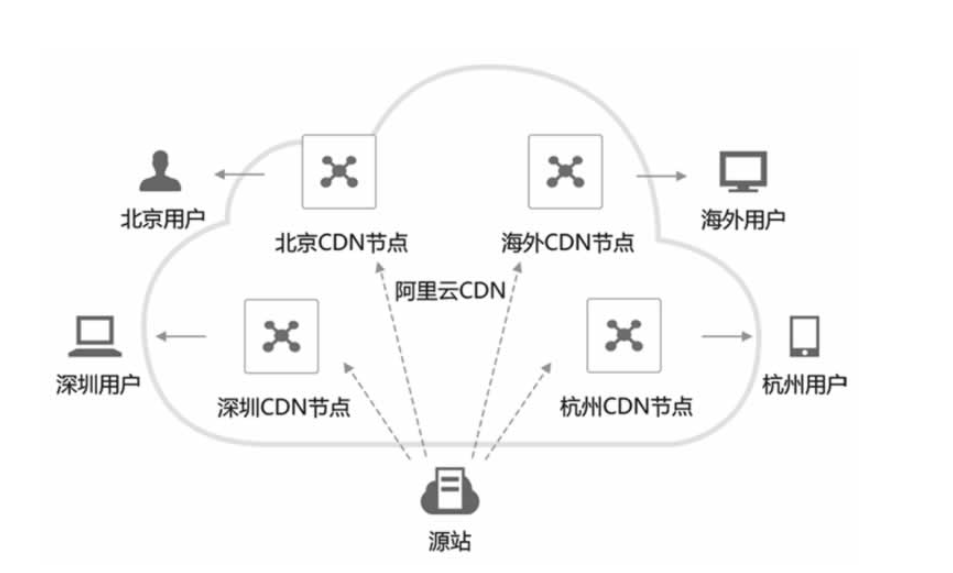
# 四.有CDN查真实IP

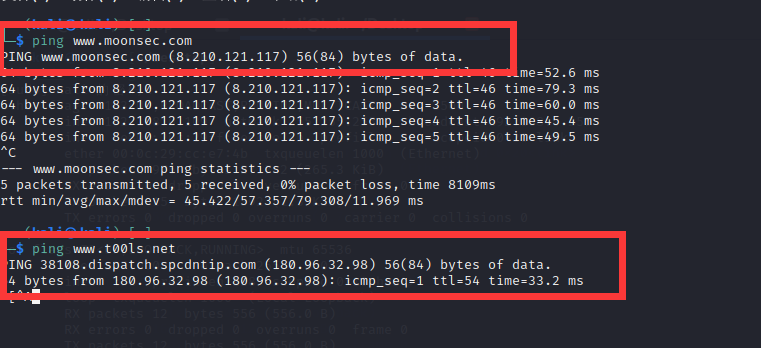
## 1 概述

目前很多网站使用了cdn服务，用了此服务 可以隐藏服务器的真实IP，加速网站静态文件的访问，而且你请求网站服务时，cdn服务会根据你所在的地区，选择合适的线路给予你访问，由此达网站加速的效果，cdn不仅可以加速网站访问，还可以提供waf服务，如防止cc攻击，SQL注入拦截等多种功能，再说使用cdn的成本不太高，很多云服务器也免费提供此服务。在进行黑盒测试的时候，往往成了拦路石，所以掌握cdn找真实ip成了不得不掌握的一项技术。



## 2 判断是否CDN

ping 域名



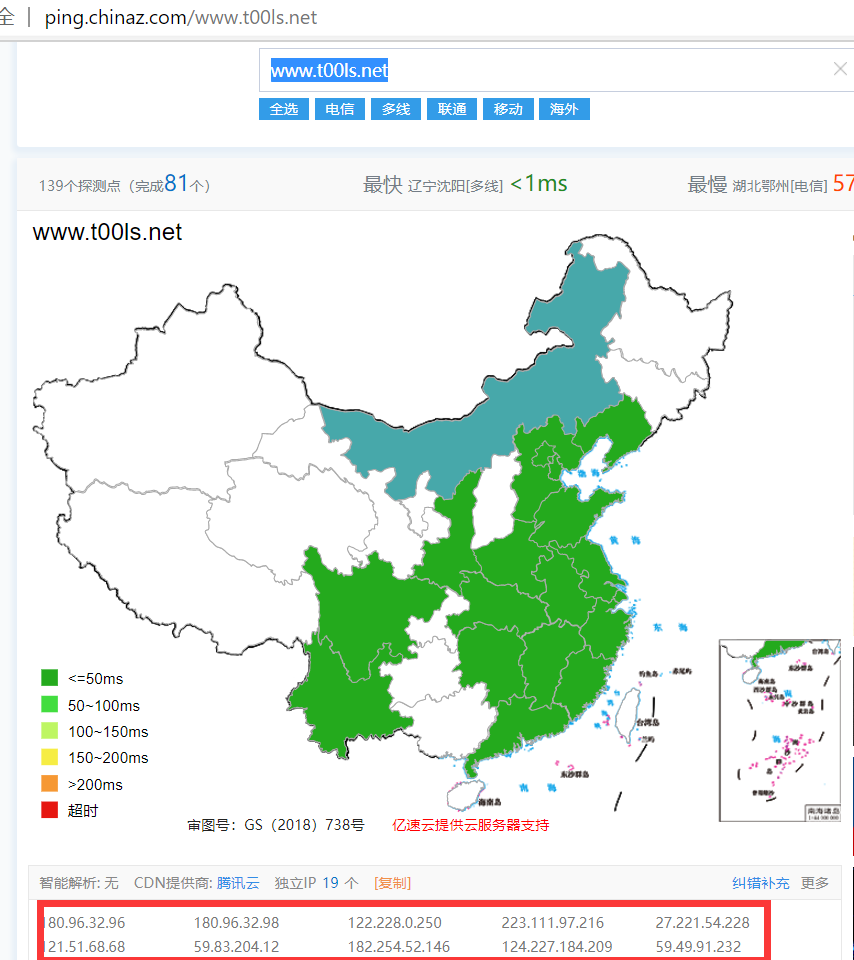
使用超级ping

<http://ping.chinaz.com/>

<http://ping.aizhan.com/>

<https://www.17ce.com/>

<http://ping.chinaz.com/www.t00ls.net>





不同的地区访问有着不同的IP，这样就确定了该域名使用了cdn了。

## 3 找真实IP的方法集合

找到真实IP可以继续旁站检测，找其他站点进行突破，也可以绕过cdn进行访问，从而绕过waf针对攻击语句的拦截 发现有攻击语句就会对攻击的IP封堵。

## 3.1 dns历史绑定记录

通过以下这些网站可以访问dns的解析，有可能存在未有绑cdn之前的记录。

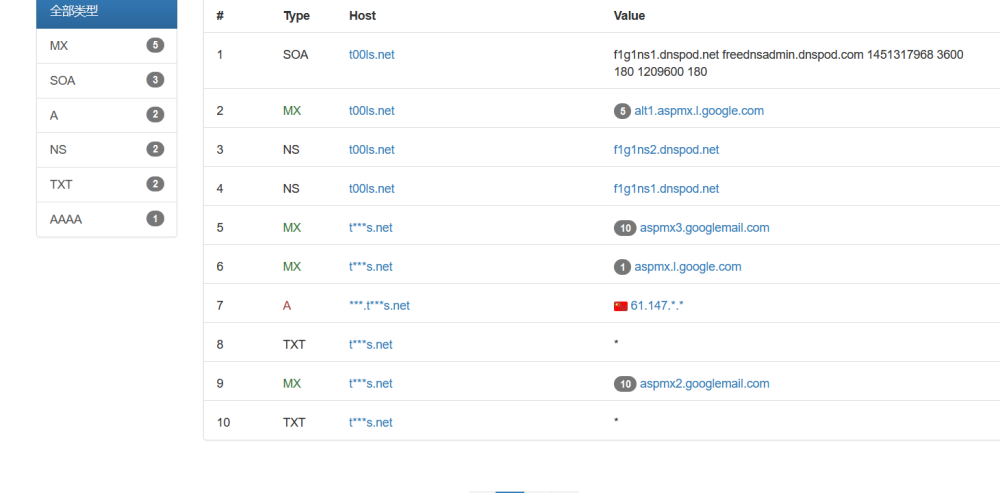
<https://dnsdb.io/zh-cn/> ###DNS查询

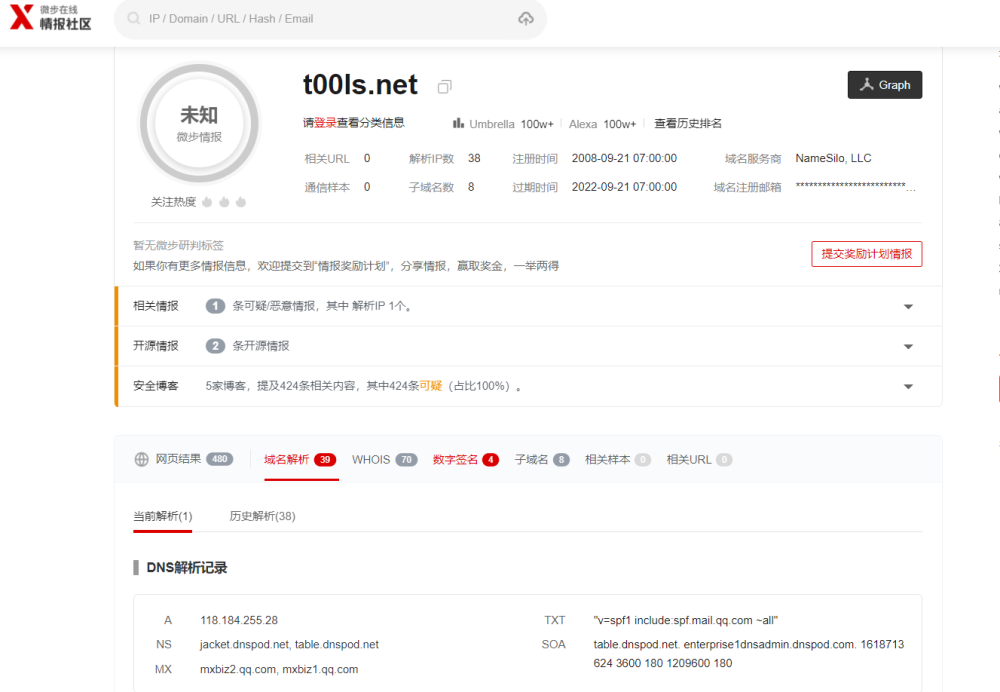
<https://x.threatbook.cn/> ###微步在线

<http://viewdns.info/> ###DNS、IP等查询

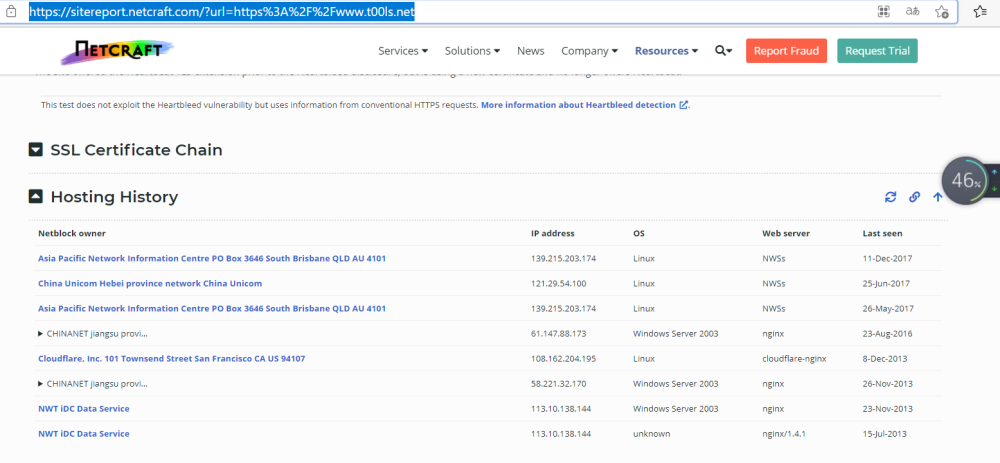
<https://tools.ipip.net/cdn.php> ###CDN查询IP

<https://sitereport.netcraft.com/?url=域名>

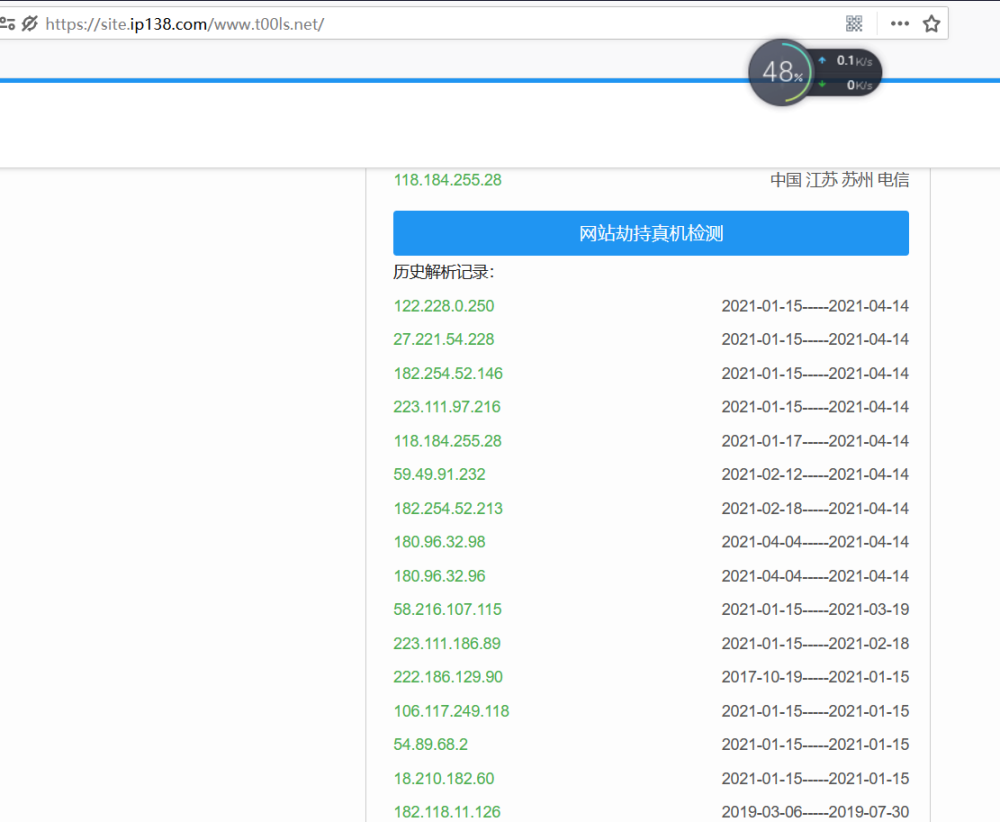




查询WWW.T00Ls.net的历史记录



<https://site.ip138.com/www.t00ls.net/>



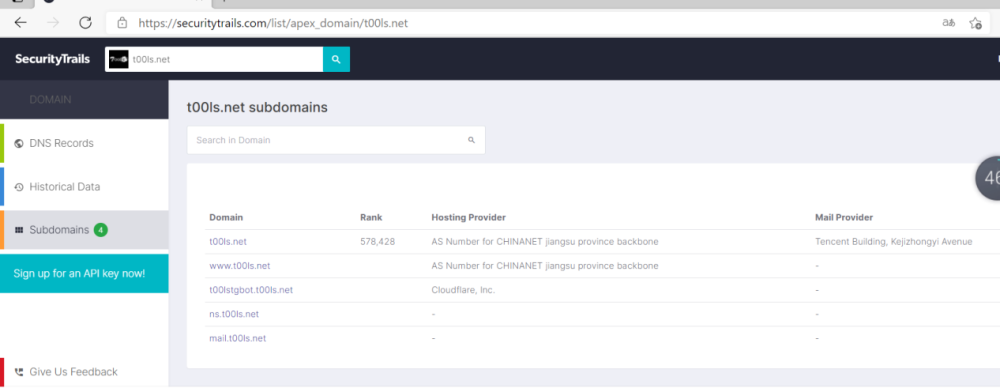
## 3.2 子域名解析

通过子域名的解析指向 也有可能指向目标的同一个IP上。

使用工具对其子域名进行穷举

在线子域名查询

<https://securitytrails.com/list/apex_domain/t00ls.net>



<http://tool.chinaz.com/subdomain/t00ls.net>

<https://phpinfo.me/domain/>

找到子域名继续确认子域名没有cdn的情况下批量进行域名解析查询，有cdn的情况继续查询历史。

域名批量解析

<http://tools.bugscaner.com/domain2ip.html>



## 3.3 国外dns获取真实IP

部分cdn只针对国内的ip访问，如果国外ip访问域名 即可获取真实IP

全世界DNS地址：

<http://www.ab173.com/dns/dns_world.php>

<https://dnsdumpster.com/>

<https://dnshistory.org/>

<http://whoisrequest.com/history/>

<https://completedns.com/dns-history/>

<http://dnstrails.com/>

<https://who.is/domain-history/>

<http://research.domaintools.com/research/hosting-history/> <http://site.ip138.com/>

<http://viewdns.info/iphistory/>

<https://dnsdb.io/zh-cn/>

<https://www.virustotal.com/>

<https://x.threatbook.cn/>

<http://viewdns.info/>

<http://www.17ce.com/>

<http://toolbar.netcraft.com/site_report?url=> <https://securitytrails.com/>

<https://tools.ipip.net/cdn.php>

## 3.4 ico图标通过空间搜索找真实ip

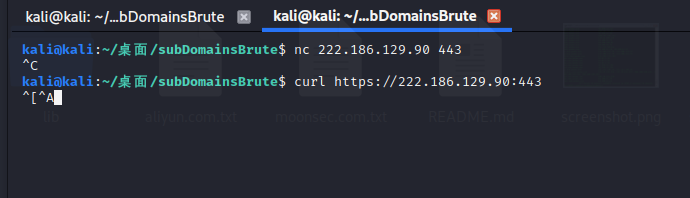
<https://www.t00ls.net/favicon.ico> 下载图标 放到fofa识别



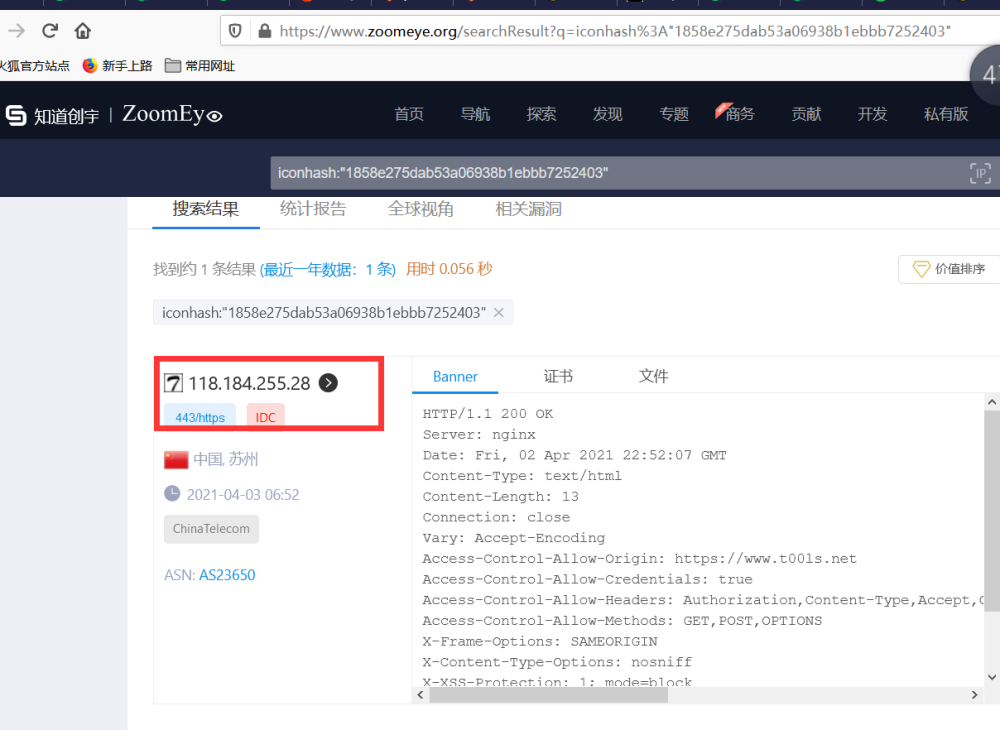
通过fofa搜图标



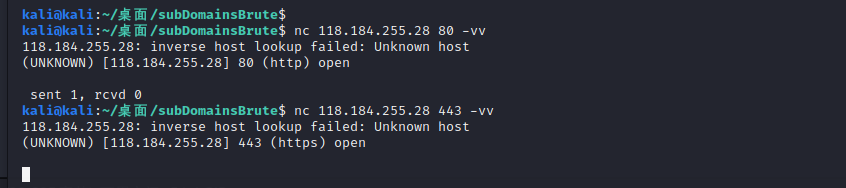
通过这样查询 快速定位资源 查看端口是否开放 这里没有开放



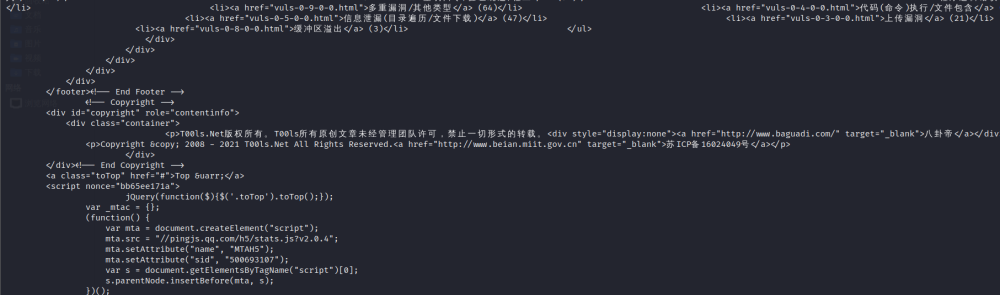
通过zoomeye搜图标



查看端口开放情况



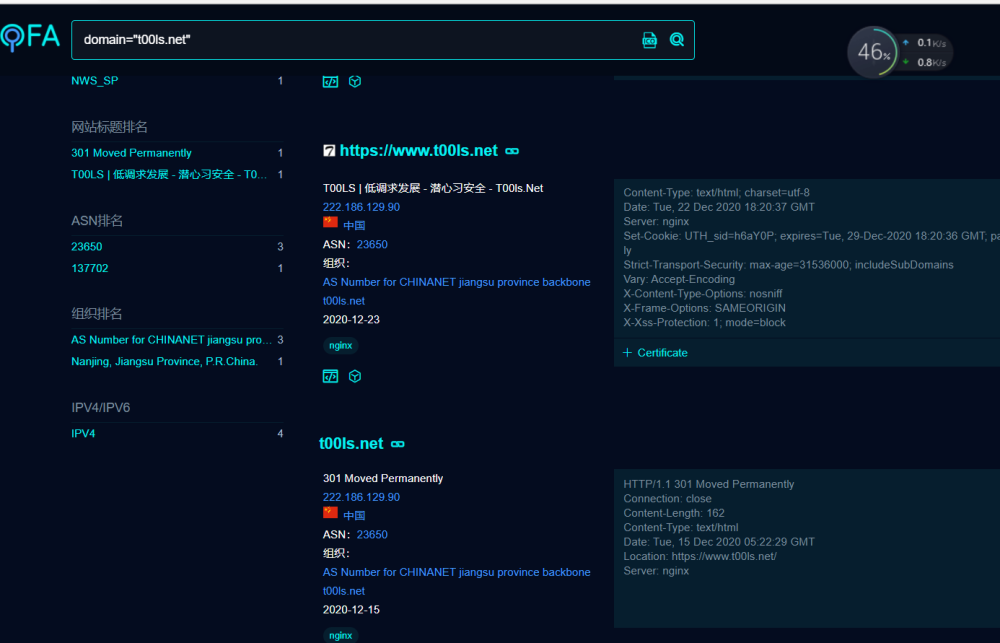
绑定hosts进行测试



这应该是真实ip了。

## 3.5 fofa搜索真实IP

domain="t00ls.net" 302一般是cdn



## 3.6 通过censys找真实ip

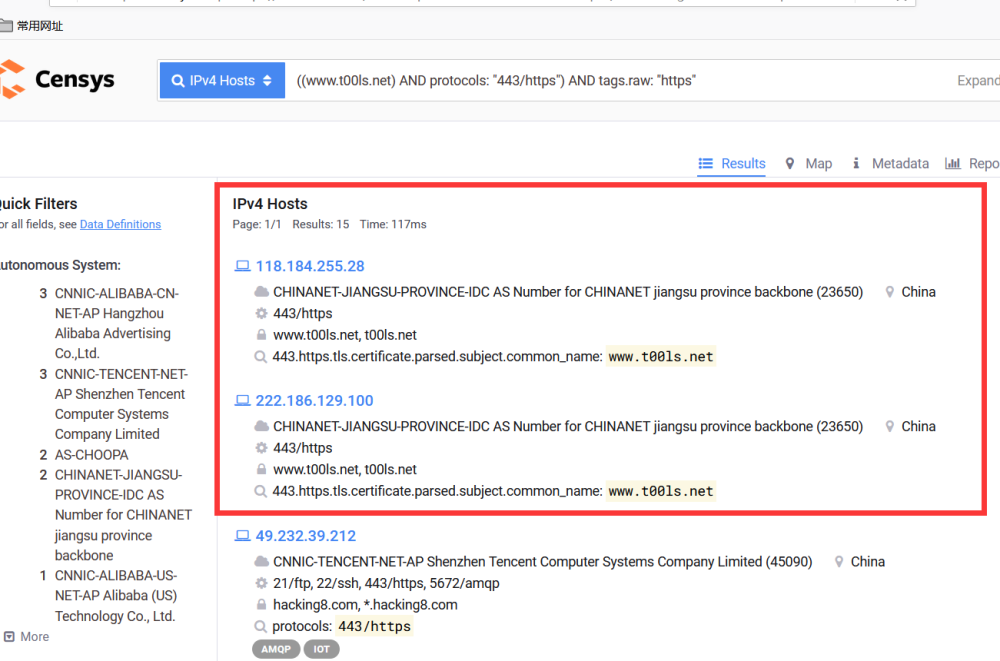
Censys工具就能实现对整个互联网的扫描，Censys是一款用以搜索联网设备信息的新型搜索引擎，能够扫描整个互联网，Censys会将互联网所有的ip进行扫面和连接，以及证书探测。

若目标站点有https证书，并且默认虚拟主机配了https证书，我们就可以找所有目标站点是该https证书的站点。

通过协议查询

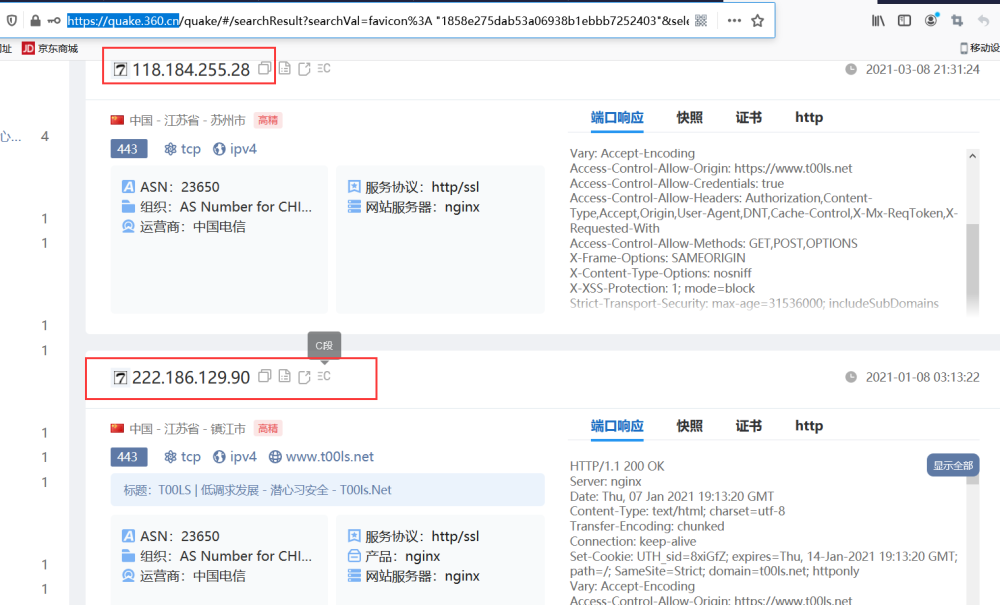
<https://censys.io/ipv4?q=((www.t00ls.net)> AND protocols: "443/https") AND tags.raw: "https"&

443.https.tls.certificate.parsed.extensions.subject\_alt\_name.dns\_names:moonsec.com



## 3.7 360测绘中心

<https://quake.360.cn>



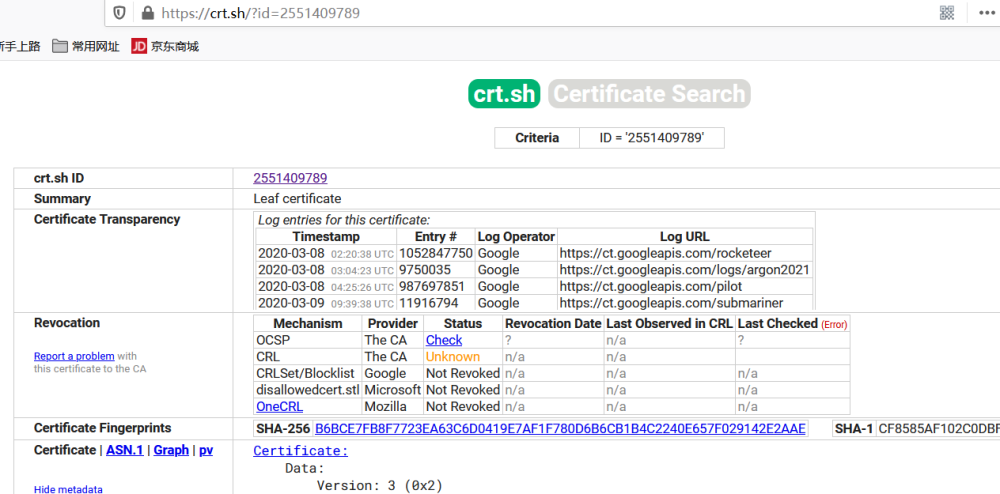
## 3.8 利用SSL证书寻找真实IP

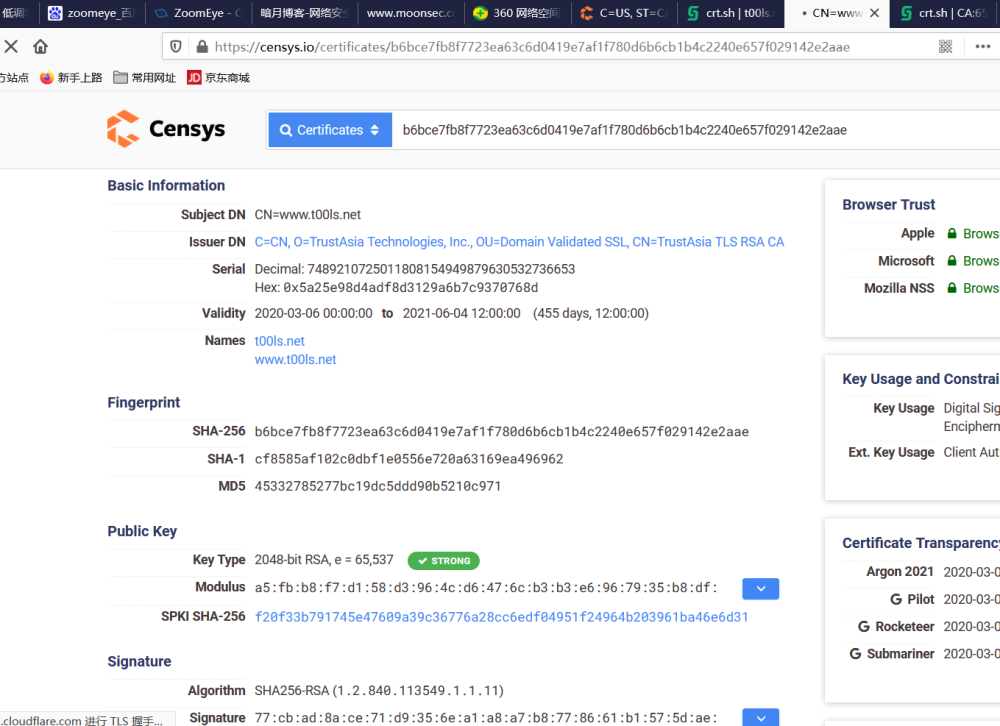
证书颁发机构(CA)必须将他们发布的每个SSL/TLS证书发布到公共日志中，SSL/TLS证书通常包含域名、子域名和电子邮件地址。因此SSL/TLS证书成为了攻击者的切入点。

获取网站SSL证书的HASH再结合Censys

利用Censys搜索网站的SSL证书及HASH，在<https://crt.sh>上查找目标网站SSL证书的HASH

再用Censys搜索该HASH即可得到真实IP地址

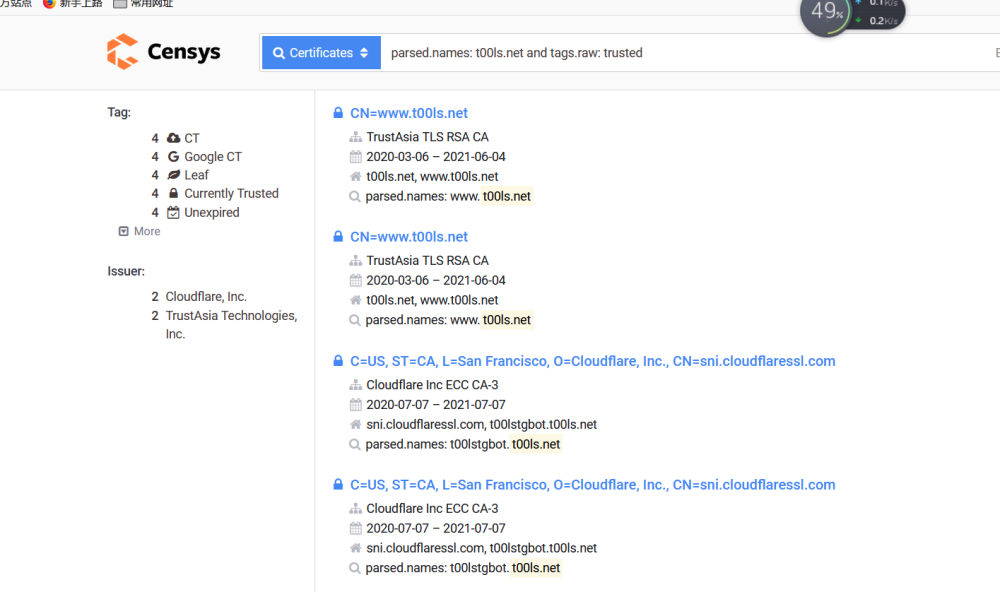




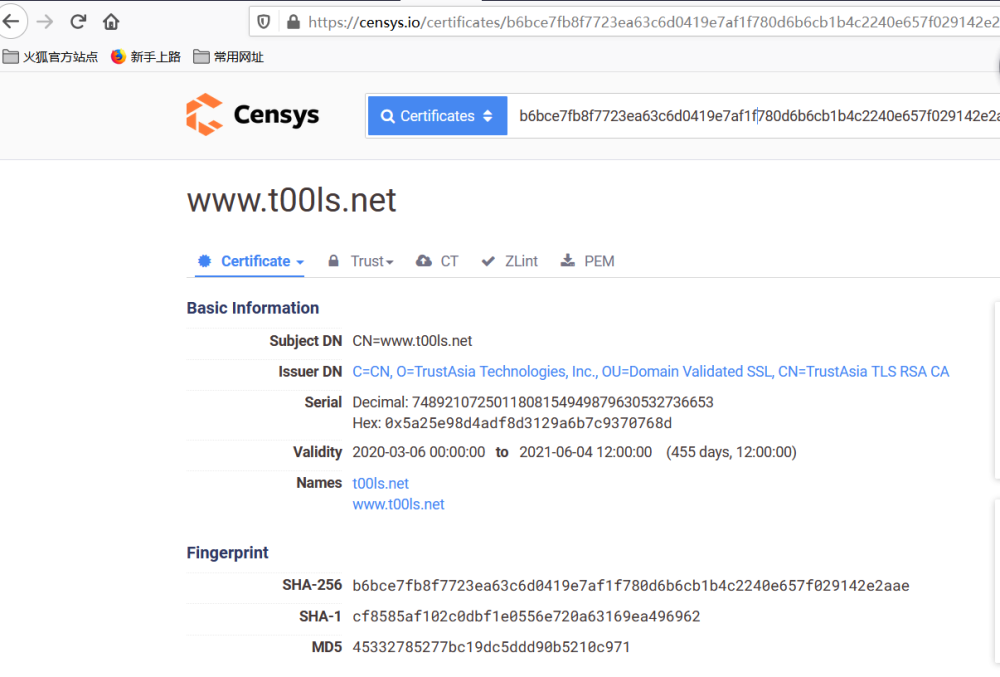
SSL证书搜索引擎：

<https://censys.io/ipv4?q=b6bce7fb8f7723ea63c6d0419e7af1f780d6b6cb1b4c2240e657f029142e2aae>

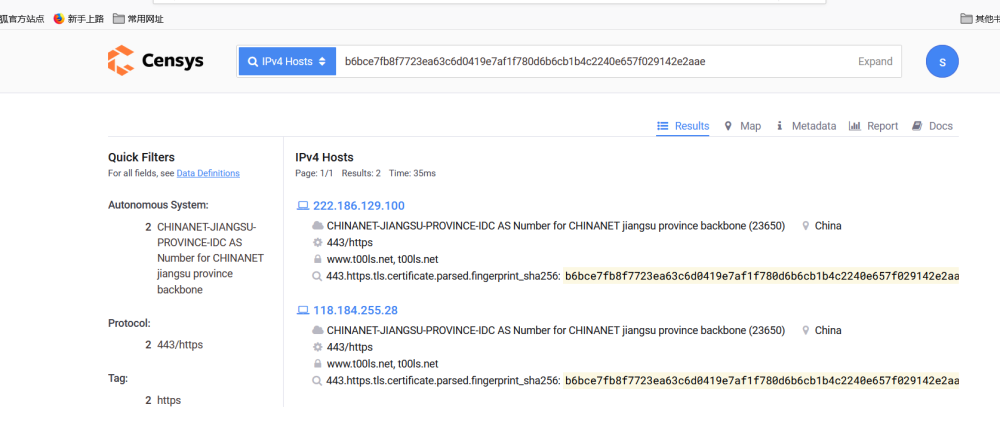
<https://censys.io/certificates?q=parsed.names%3A+t00ls.net+and+tags.raw%3A+trusted>



找到hash



转成ipv4 进行搜索



找到两个IP

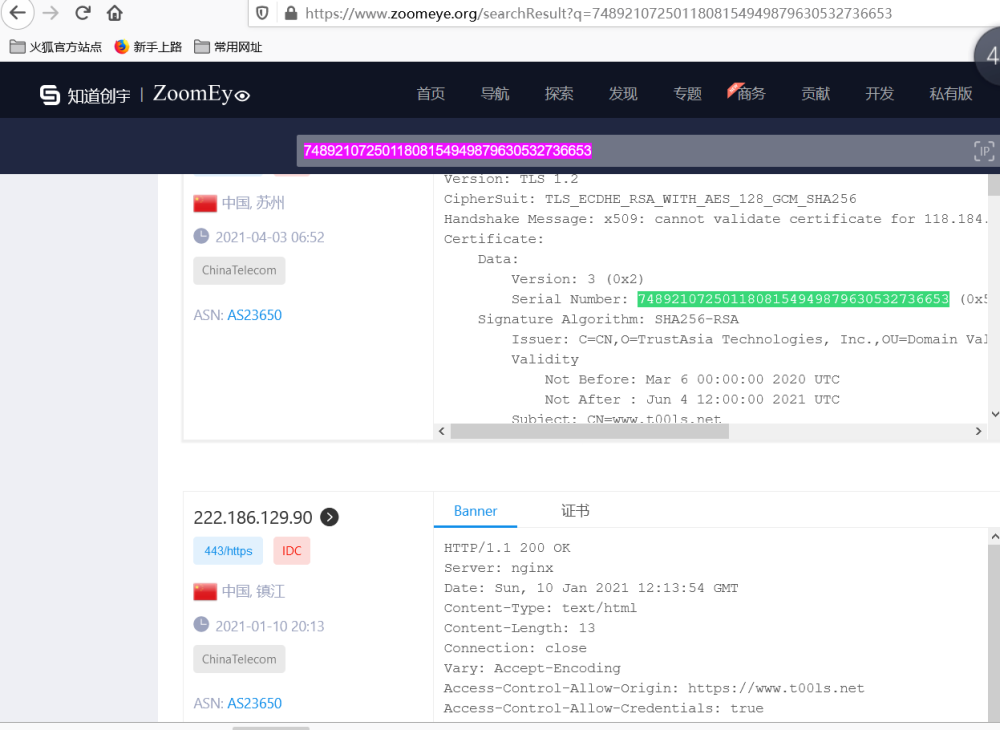
两个ip

222.186.129.100

118.184.255.28

或者把hash放进网络空间搜索

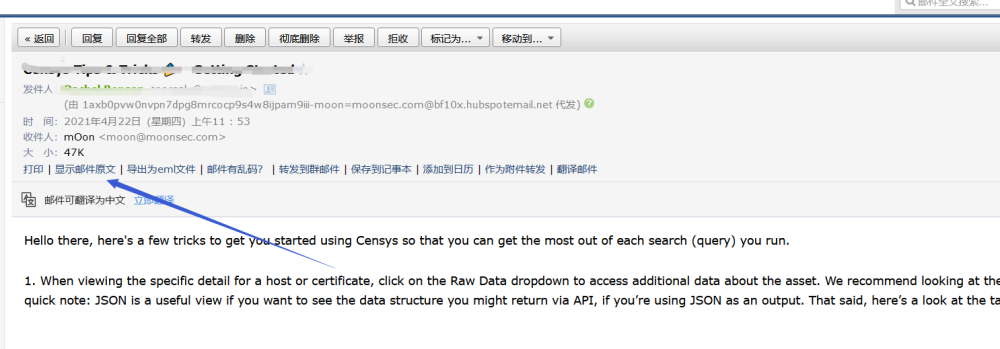
7489210725011808154949879630532736653



成功找到网络IP 接着就是判断ip是否是这个域名的了。

## 3.9 邮箱获取真实IP

网站在发信的时候，会附带真实的IP地址 进入邮箱 查看源文件头部信息 选择from





是否真实 还需要 邮箱发送是否与网站同一个IP地址。

## 3.10 网站敏感文件获取真实IP

* 文件探针

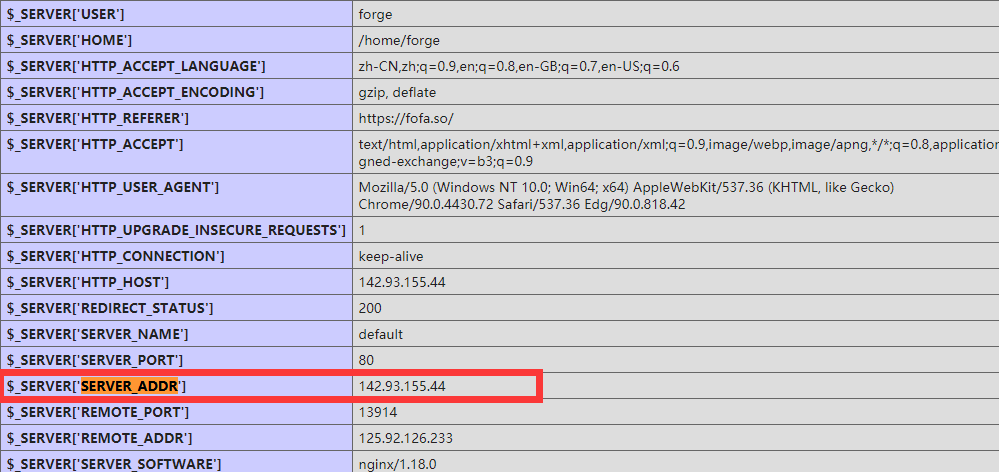
* phpinfo

* 网站源代码

* 信息泄露

* GitHub信息泄露

* js文件



## 3.11 F5 LTM解码法

当服务器使用F5 LTM做负载均衡时，通过对set-cookie关键字的解码真实ip也可被获取，

例如：Set-Cookie: BIGipServerpool\_8.29\_8030=487098378.24095.0000，先把第一小

节的十进制数即487098378取出来，然后将其转为十六进制数1d08880a，接着从后至前，

以此取四位数出来，也就是0a.88.08.1d，最后依次把他们转为十进制数10.136.8.29，也就

是最后的真实ip。

rverpool-cas01=3255675072.20480.0000; path=/

3255675072 转十六进制 c20da8c0 从右向左取 c0a80dc2 转10进制 192 168 13 194

## 3.12 APP获取真实IP

如果网站有app，使用Fiddler或BurpSuite抓取数据包 可能获取真实IP

模拟器 mimi模拟器抓包

## 3.13 小程序获取真实IP

## 3.14 配置不当获取真实IP

在配置CDN的时候，需要指定域名、端口等信息，有时候小小的配置细节就容易导致CDN防护被绕过。

* 案例1：为了方便用户访问，我们常常将www.test.com 和 test.com 解析到同一个站点，而CDN只配置了www.test.com，通过访问test.com，就可以绕过 CDN 了。

* 案例2：站点同时支持http和https访问，CDN只配置 https协议，那么这时访问http就可以轻易绕过。

## 3.15 banner

获取目标站点的banner，在全网搜索引擎搜索，也可以使用AQUATONE，在Shodan上搜索相同指纹站点。

可以通过互联网络信息中心的IP数据，筛选目标地区IP，遍历Web服务的banner用来对比CDN站的banner，可以确定源IP。

欧洲：

<http://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest>

北美：

<https://ftp.arin.net/pub/stats/arin/delegated-arin-extended-latest>

亚洲：

ftp://ftp.apnic.net/public/apnic/stats/apnic/delegated-apnic-latest

非洲：

ftp://ftp.afrinic.net/pub/stats/afrinic/delegated-afrinic-latest

拉美：

ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-extended-latest

获取CN的IP

<http://www.ipdeny.com/ipblocks/data/countries/cn.zone>

例如：

找到目标服务器 IP 段后，可以直接进行暴力匹配 ，使用zmap、masscan 扫描 HTTP banner，然后匹配到目标域名的相同 banner

zmap -p 80 -w bbs.txt -o 80.txt

使用zmap的banner-grab对扫描出来80端口开放的主机进行banner抓取。

cat /root/bbs.txt |./banner-grab-tcp -p 80 -c 100 -d http-req -f ascii > http-banners.out

根据网站返回包特征，进行特征过滤

location: plugin.php?id=info:index

<https://fofa.so/>

title="T00LS | 低调求发展 - 潜心习安全 - T00ls.Net"

<https://www.zoomeye.org/>

title:"T00LS | 低调求发展 -潜心习安全 -T00ls.Net"

<https://quake.360.cn/>

response:"T00LS | 低调求发展 - 潜心习安全 - T00ls.Net"

1、ZMap号称是最快的互联网扫描工具，能够在45分钟扫遍全网。<https://github.com/zmap/zmap>

2、Masscan号称是最快的互联网端口扫描器，最快可以在六分钟内扫遍互联网。

<https://github.com/robertdavidgraham/masscan>

## 3.16 长期关注

在长期渗透的时候，设置程序每天访问网站，可能有新的发现。每天零点 或者业务需求增大 它会换ip 换服务器的。

## 3.17 流量攻击

发包机可以一下子发送很大的流量。

这个方法是很笨，但是在特定的目标下渗透，建议采用。

cdn除了能隐藏ip，可能还考虑到分配流量，

不设防的cdn 量大就会挂，高防cdn 要大流量访问。

经受不住大流量冲击的时候可能会显示真实ip。

站长->业务不正常->cdn不使用->更换服务器。

## 3.18 被动获取

被动获取就是让服务器或网站主动连接我们的服务器，从而获取服务器的真实IP

如果网站有编辑器可以填写远程url图片，即可获取真实IP

如果存在ssrf漏洞 或者xss 让服务器主动连接我们的服务器 均可获取真实IP。

## 3.19 扫全网获取真实IP

<https://github.com/superfish9/hackcdn>

<https://github.com/boy-hack/w8fuckcdn>