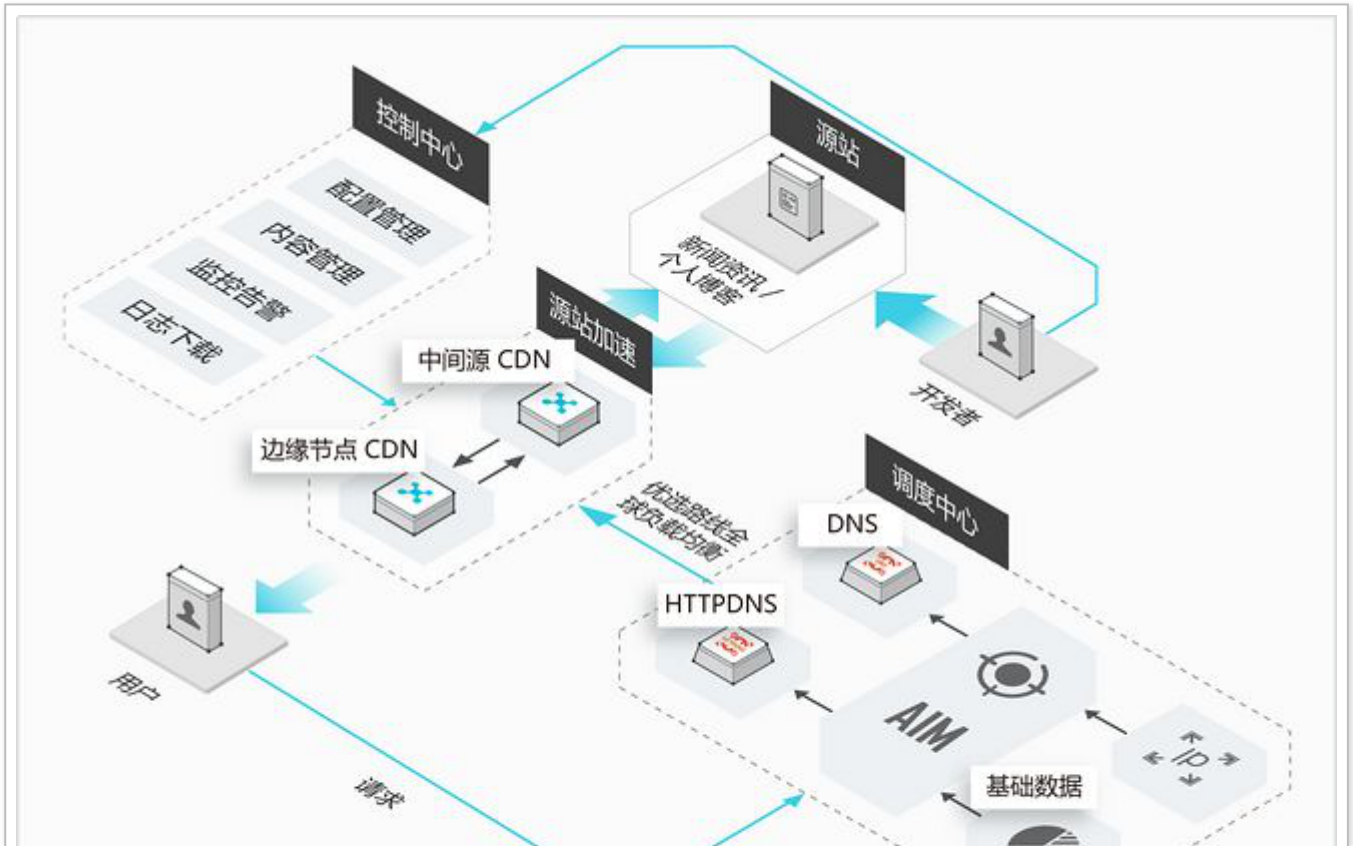
绕过 CDN 查找真实 IP 方法总结

0x00 CDN 简述

CDN 的全称是 Content Delivery Network，即内容分发网络。CDN 是构建在现有网络基础之上的智能虚拟网络，依靠部署在各地的边缘服务器，通过中心平台的负载均衡、内容分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。

百度百科



0x01 域名解析过程

- 传统访问：用户访问域名 --> 解析 IP--> 访问目标主机
- 简单模式：用户访问域名 -->CDN 节点 --> 真实 IP--> 目标主机
- 360 网站卫士：用户访问域名 -->CDN 节点（云 WAF）--> 真实 IP--> 目标主机

注：目前市面上大多数的 CDN 服务商都提供了云 WAF 配置选项，内置了多种安全防护策略，可对 SQL 注入、XSS 跨站、Webshell 上传、后门隔离保护、命令注入、恶意扫描等攻击行为进行有效拦截。

0x02 CDN 配置方法

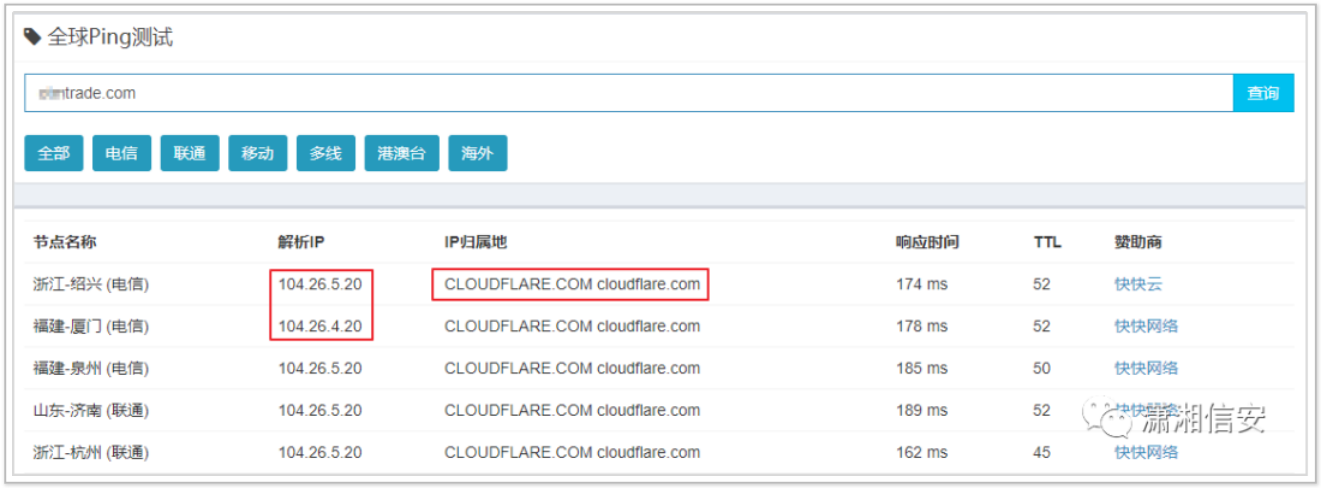
- 将域名的 NS 记录指向 CDN 厂商提供的 DNS 服务器。
- 给域名设置一个 cname 记录，将它指向 CDN 厂商提供的另一个域名。

0x03 CDN 检测方法

利用“全球 Ping”快速检测目标是否存在 CDN，如果得到的 IP 归属地是某 CDN 服务商，或者每个地区得到的 IP 地址都不一样则说明可能存在 CDN，可用以下几个网站检测！

```
https://wepcc.com
http://ping.chinaz.com
https://asm.ca.com/en/ping.php
```

注：全球 Ping 有一定机率可以得到目标服务器真实 IP，因为有的 CDN 服务商可能没有某些地区的 CDN 节点。



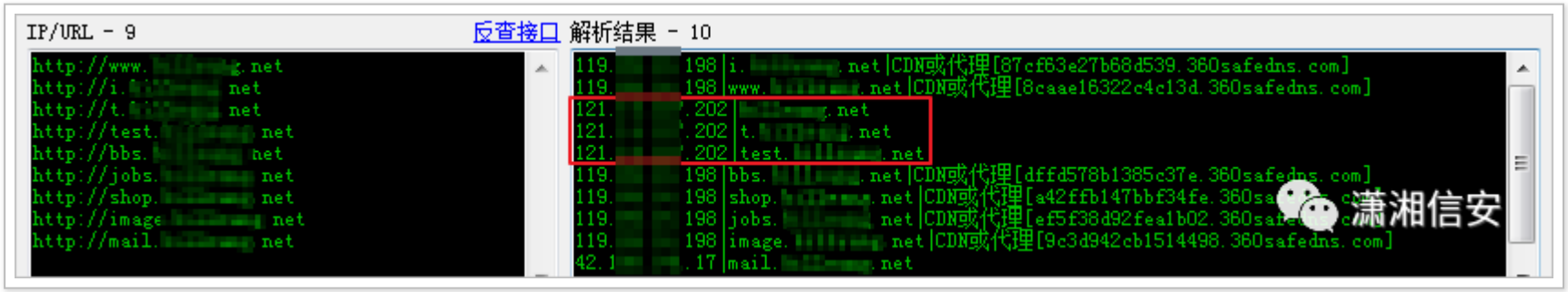
0x04 查找真实 IP 方法

(1) phpinfo 等探针找到真实 IP

通过 l.php、phpinfo.php 等这类探针文件即可得到真实 IP 地址，phpinfo.php 搜索 SERVER_NAME。

(2) 网站根域或子域找到真实 IP

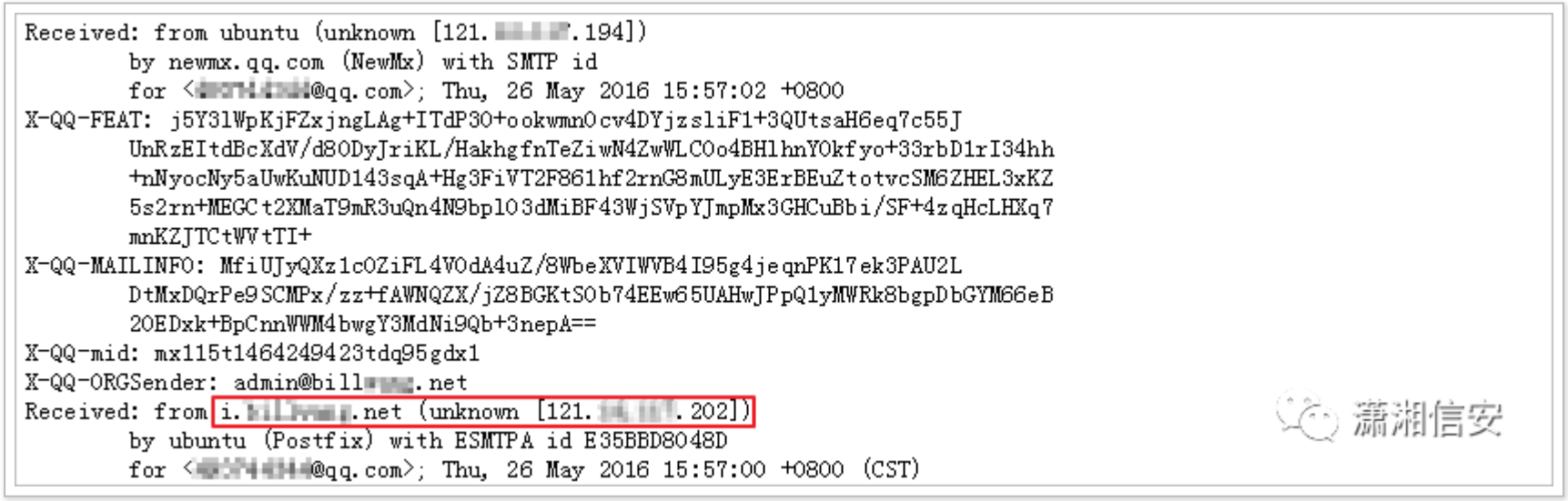
大部分 CDN 服务都是按流量进行收费的，所以一些网站管理员只会给重要业务部署 CDN，也有很多人会忘了给顶级域名部署 CDN，所以尽可能的多去搜集一些子域名能提高找到真实 IP 地址的机率。



注：有时多个子域名可能不会解析到同一台服务器，而是根据公司业务的重要与非重要性将子域名解析在内网或外网的不同服务器中，需要有一定的分析能力。

(3) 利用邮件服务器找到真实 IP

Web 和 Email 属同服务器时可以通过 Email 来查询目标真实 IP 地址，如果 Web 和 Email 属不同服务器时我们通过 Email 得到的可能只是邮件服务器的 IP 地址，所以在 hosts 文件中绑定真实 IP 后无法访问目标网站也属正常现象。常见发送邮件的功能有：注册用户、找回密码等。

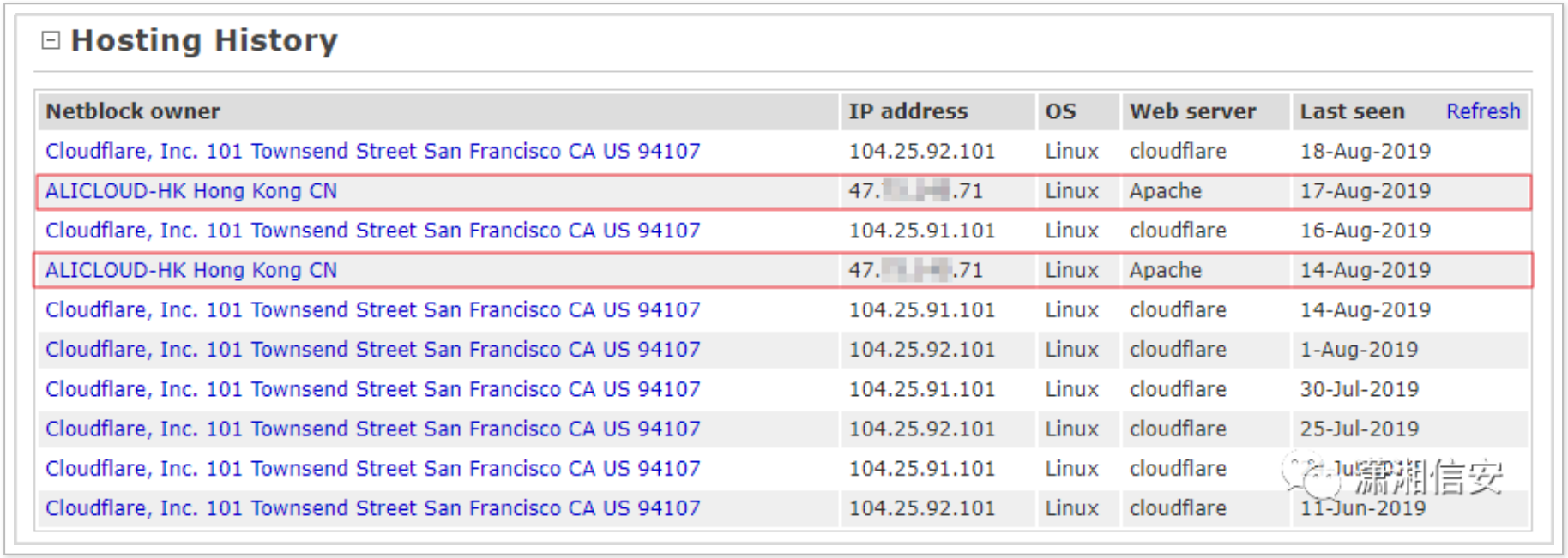


(4) 域名历史解析记录找到真实 IP

通过查询目标域名历史解析记录可能会找到部署 CDN 前的解析记录（真实 IP 地址），可以用以下几个网站来查询。

```
https://domain.8aq.net    //基于Rapid7 Open Data
https://x.threatbook.cn

https://webiplookup.com
https://viewdns.info/iphistory
https://securitytrails.com/#search
https://toolbar.netcraft.com/site_report
```

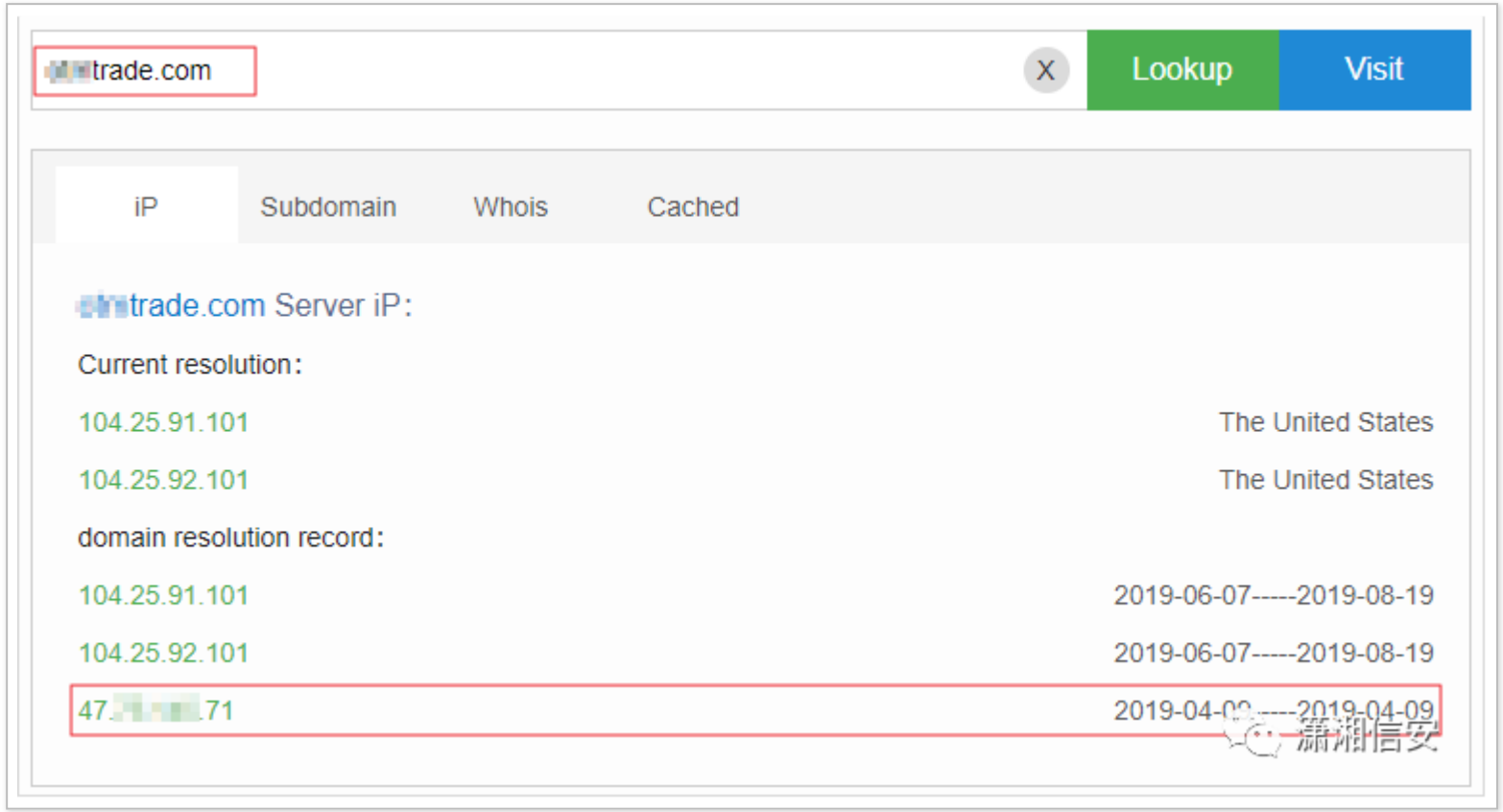


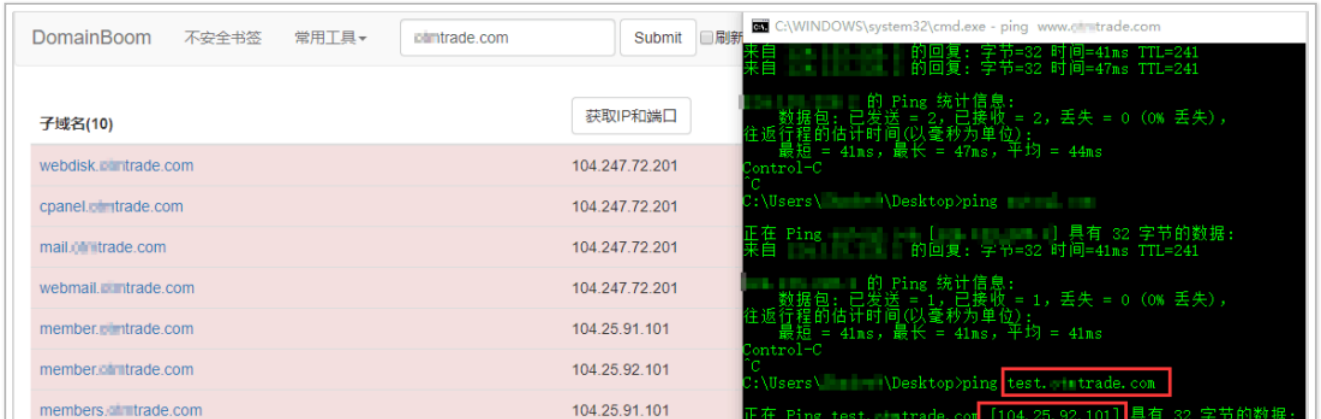
Hosting History

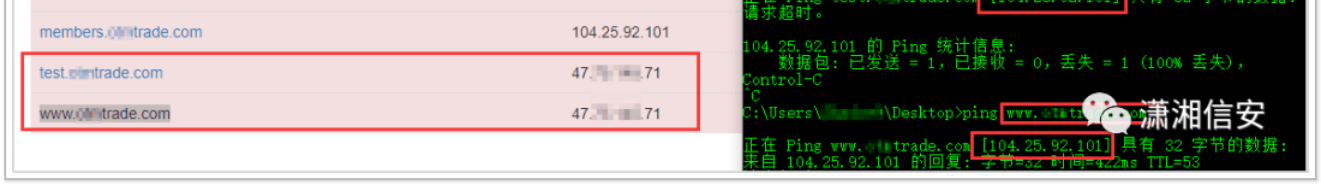
Netblock owner	IP address	OS	Web server	Last seen Refresh
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.25.92.101	Linux	cloudflare	18-Aug-2019
ALICLOUD-HK Hong Kong CN	47.[redacted].71	Linux	Apache	17-Aug-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.25.91.101	Linux	cloudflare	16-Aug-2019
ALICLOUD-HK Hong Kong CN	47.[redacted].71	Linux	Apache	14-Aug-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.25.91.101	Linux	cloudflare	14-Aug-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.25.92.101	Linux	cloudflare	1-Aug-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.25.91.101	Linux	cloudflare	30-Jul-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.25.92.101	Linux	cloudflare	25-Jul-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.25.91.101	Linux	cloudflare	[illegible]Jul-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.25.92.101	Linux	cloudflare	11-Jun-2019

IP history results for [redacted]trade.com.
==========

IP Address	Location	IP Address Owner	Last seen on this IP
104.25.92.101	United States	Cloudflare, Inc.	2019-08-18
104.25.91.101	United States	Cloudflare, Inc.	2019-08-18
47.[redacted].71	Beijing - China	Alibaba.com LLC	2019-05-23
104.25.92.101	United States	Cloudflare, Inc.	2019-05-22
104.25.91.101	United States	Cloudflare, Inc.	2019-05-22
47.[redacted].71	Beijing - China	Alibaba.com LLC	2019-05-01
104.25.92.101	United States	Cloudflare, Inc.	2019-04-30
104.25.91.101	United States	Cloudflare, Inc.	2019-04-30
47.[redacted].71	Beijing - China	Alibaba.com LLC	2019-04-22
47.52.193.157	Hong Kong	Alibaba.com LLC	2018-11-27
184.168.221.47	Scottsdale - United States	GoDaddy.com, LLC	2018-09-02


trade.com
X
Lookup
Visit
iP
Subdomain
Whois
Cached
trade.com Server iP:
Current resolution:
104.25.91.101
The United States
104.25.92.101
The United States
domain resolution record:
104.25.91.101
2019-06-07-----2019-08-19
104.25.92.101
2019-06-07-----2019-08-19
47.71
2019-04-09-----2019-04-09


DomainBoom
不安全书签
常用工具
trade.com
Submit
子域名(10)
获取IP和端口
webdisk.trade.com
104.247.72.201
cpanel.trade.com
104.247.72.201
mail.trade.com
104.247.72.201
webmail.trade.com
104.247.72.201
member.trade.com
104.25.91.101
member.trade.com
104.25.92.101
members.trade.com
104.25.91.101
C:\WINDOWS\system32\cmd.exe - ping www.trade.com
的回复: 字节=32 时间=41ms TTL=241
的回复: 字节=32 时间=47ms TTL=241
的 Ping 统计信息:
数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 41ms, 最长 = 47ms, 平均 = 44ms
Control-C
^C
C:\Users\ \Desktop>ping
正在 Ping [ ] 具有 32 字节的数据:
的回复: 字节=32 时间=41ms TTL=241
的 Ping 统计信息:
数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 41ms, 最长 = 41ms, 平均 = 41ms
Control-C
^C
C:\Users\ \Desktop>ping test.trade.com
[104.25.92.101] 具有 32 字节的数据:



(5) FOFA 查询网站标题找到真实 IP

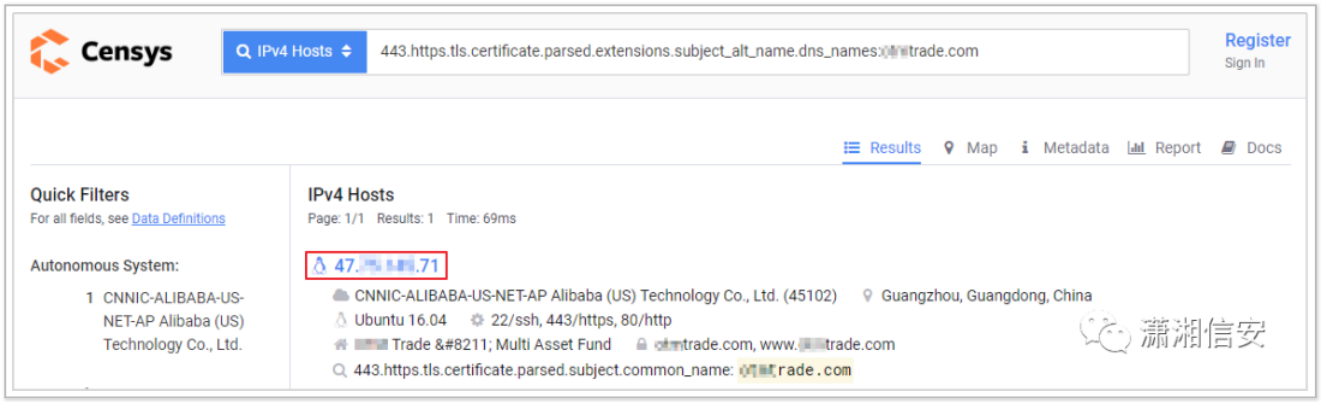
利用“FOFA 网络空间安全搜索引擎”搜索目标网站源代码中的 title 标签内容即可得到真实 IP 地址。

```
title="*** ***** – Multi Asset Fund"
```

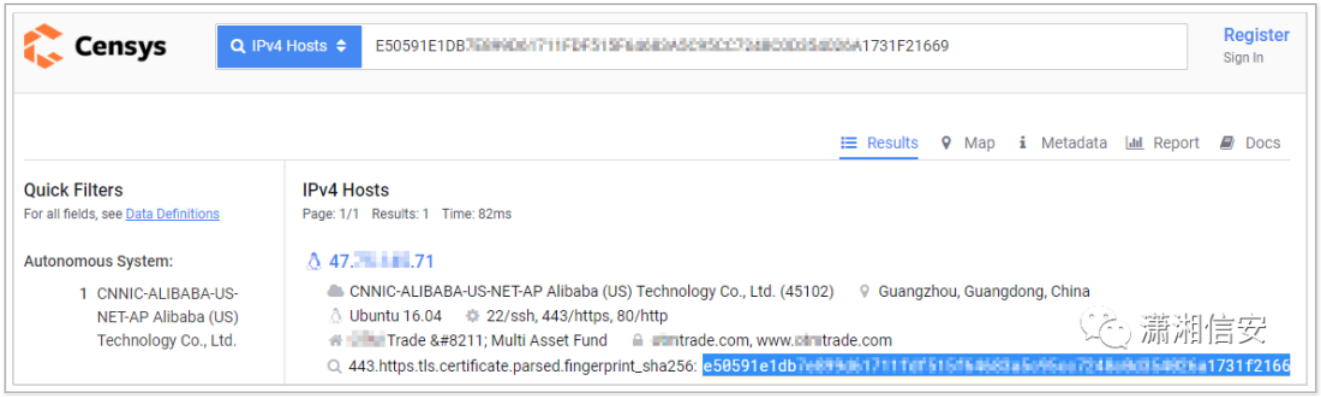
(6) Censys 查询 SSL 证书找到真实 IP

利用“Censys 网络空间搜索引擎”搜索目标域名的 SSL 证书和 HASH，https://crt.sh 上查找他 SSL 证书的 HASH，然后再用 Censys 搜索该 HASH 值即可得到真实 IP 地址。

```
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names:***trade.com
```



crt.sh ID	
Summary	Leaf certificate
Certificate Transparency	Timestamp / Entry # / Log Operator / Log URL
	2019-11-01 10:54:16 UTC / 84711472 / Google / https://ct.googleapis.com/logs/argon2020
	2019-11-01 10:54:16 UTC / 36765924 / Google / https://ct.googleapis.com/logs/xenon2020
	2019-11-01 10:54:16 UTC / 71386494 / Let's Encrypt / https://oak.ct.letsencrypt.org/2020
Revocation	Mechanism / Provider / Status / Revocation Date / Last Observed in CRL / Last Checked (Error)
Report a problem with this certificate to the CA	OCSP / The CA / Check / ? / n/a / ?
	CRL / The CA / Unknown / n/a / n/a /
	CRLSet/Blacklist / Google / Not Revoked / n/a / n/a / n/a
	disallowedcert.stl / Microsoft / Not Revoked / n/a / n/a / n/a
	OneCRL / Mozilla / Not Revoked / n/a / n/a / n/a
SHA-256(Certificate)	E50591E1DB 1731F21669
SHA-1(Certificate)	



(7) 通过分析目标 C 段来判断真实 IP

这种方法得看目标有多少子域名吧，如果子域够多，且又有多台服务器（同段），找一个没有部署 CDN 的子域名，然后扫描整个 C 段查找与目标站 Title 一致的即可找到他的真实 IP 地址！

目标站 111.test.com 解析在 192.168.1.10，title：90sec 社区，通过 333.test.com 子域名得到 333 真实 IP 地址 192.168.1.12，然后扫描整个 C 段，当扫到 192.168.1.10 这个 IP 时发现一个 title 同为“90sec 社区”的网站，域名也是 111.test.com，这样就能确定 192.168.1.10 为真实 IP 了。

网站域名	域名解析 IP	CDN 节点 IP
111.test.com（目标）	192.168.1.10	8.8.8.8
222.test.com	192.168.1.11	9.9.9.9
333.test.com	192.168.1.12	没有 CDN

(8) 自建 CDN 节点服务器找到真实 IP

这篇笔记当时没有记录下来，其实就是 MS17-010 刚出来时很多机器都还没打补丁，在批量过程中打了一台别人自建的 CDN 节点服务器，然后在里边发现很多解析到这边的 IP 地址，其实这些 IP 地址就是某些网站的真实 IP，所以这也算是一种思路吧，但是得先拿到 CDN 节点服务器权限。或者可以通过 DDOS 攻击方式将其流量耗尽后即会显示真实 IP，因为免费和自建 CDN 的流量都不会很多。

(9) 通过目标网站的漏洞找到真实 IP

Web 安全漏洞：XSS、SSRF、命令执行、文件上传等，但可能需要先绕过云 WAF 安全防护。
敏感信息泄露：Apache status、Jboss status、SVN、Github 等敏感信息和网页源代码泄露。

(10) 通过社工 CDN 控制台找到真实 IP

通过社会工程学将搜集到的信息组合生成用户名和密码字典对 CDN 控制台进行爆破或者手工尝试，但是得在没有验证码和登录次数限制的情况下，然后找到他的真实解析 IP 地址。

(11) Zmap 全网扫描及 F5 LTM 解码法

这两种方法都是前辈们以前写的，个人感觉较为复杂，并没有亲自实践过，不知是否真的可行?

注意事项：

部署 CDN 的网站有必要设置严格访问控制策略，仅允许 CDN 节点访问网站真实服务器 80 端口，这样设置的好处就是即使在 hosts 文件中绑定了真实 IP 后仍然无法访问。
笔者曾经在一次渗透测试过程中就遇到过类似情况，就是成功绑定了真实 IP 后，虽然能够正常访问到目标网站，但是仍然没有绕过云 WAF，具体情况有点记不太清了，当时没有去细研究这个问题!
潇湘信安 发起了一个读者讨论 有没有表哥补充下自己用过的其他方法? 精选讨论内容

有篇文章写过，思路是可行的，就是比较耗时!