

## 0x01 前言

垂直关联 — 从根域查找子域的过程。这是挖掘漏洞赏金的第二步，第一步从上一篇文章水平关联开始，了解的资产越多，您可以攻击的资产就越多，通过扩大攻击面，您更有可能发现漏洞。

## 0x02 查找子域名

我找到几种查找子域名的方法：

### 工具被动查找子域名

测试的工具：

- Anubis
- Amass
- Subfinder
- TheHarvester
- OneForAll
- BBOT

测试规则：

目标：tesla.com

免费API，不用任何付费的API。

在同一台VPS上进行测试，每个工具单独运行。

### Subfinder



```
1 subfinder -domain tesla.com -all -t 100
```

<https://github.com/projectdiscovery/subfinder>

**版本:** v2.5.7 (18 三月 2023)

**子域:** 616

**运行时间:** 30 秒

## oneforall

```
1 python oneforall.py --target tesla.com --req False run
```

https://github.com/shmilylty/OneForAll

版本: v0.4.5 (10 七月 2022)

子域: 424

运行时间: 1 分 55 秒

开始 分割 00:01:55.414 清除

1 停止: 00:01:55.414

```

14:37:24,332 [INFOR] resolve:143 - Start resolving subdomains of tes
14:37:24,346 [INFOR] resolve:166 - Running massdns to resolve subdom
14:37:27,106 [INFOR] resolve:104 - Processing resolved results
14:37:27,167 [INFOR] resolve:172 - Finished resolve subdomains of te
14:37:27,168 [INFOR] resolve:61 - Saving resolved results
14:37:27,200 [ALERT] export:66 - The subdomain result for tesla.com:
la.com.csv
14:37:27,202 [INFOR] oneforall:255 - Finished OneForAll

```

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
397	1064			1	http://vehicle-files.eng.euw1.vn.	vehicle-files.eng.euw1.vn.c		5	e92385.dsc	23.44.51.170,23.44.51.146		80		OK		
398	1086			1	http://vehicle-files.eng.usw2.vn.	vehicle-files.eng.usw2.vn.c		5	e29246.dsc	104.123.70.9,104.123.70.81		80		OK		
399	1159			1	http://vehicle-files.prd.euw1.vn.	vehicle-files.prd.euw1.vn.c		5	e73066.dsc	2.16.187.139,2.16.187.11		80		OK		
400	1156			1	http://vehicle-files.prd.usw2.vn.	vehicle-files.prd.usw2.vn.c		5	e132349.dsc	23.43.85.10,23.43.85.16		80		OK		
401	407			1	http://view.email.tesla.com	view.email.tesla.com		2	view.virt	136.147.129.32		80		OK		
402	557			1	http://view.emails.tesla.com	view.emails.tesla.com		2	view.email	13.111.49.179		80		OK		
403	95			1	http://vmanage-alerts.tesla.com	vmanage-alerts.tesla.com		1	e1792.dsc	184.27.16.62		80		OK		
404	365			1	http://vpn1.tesla.com	vpn1.tesla.com		1	vpn1.tesla	8.45.124.215		80		OK		
405	339			1	http://vpn2.tesla.com	vpn2.tesla.com		1	vpn2.tesla	8.47.24.215		80		OK		
406	104			1	http://vpn3.tesla.com	vpn3.tesla.com		1	vpn3.tesla	8.21.14.215		80		OK		
407	423			1	http://warehouse-stg.tesla.com	warehouse-stg.tesla.com		1	warehouse	199.66.9.83		80		OK		
408	376			1	http://warehouse.tesla.com	warehouse.tesla.com		1	e1792.dsc	23.52.120.69		80		OK		
409	1652			1	http://warp.tesla.com	warp.tesla.com		1	e1792.dsc	184.27.16.62		80		OK		
410	165			1	http://wdm.kronos.tesla.com	wdm.kronos.tesla.com		2	kronos-wdm	52.38.42.230,44.227.162.90,52.		80		OK		
411	326			1	http://wim.kronos.tesla.com	wim.kronos.tesla.com		2	wim.kronos	217.138.108,23.202.231.167		80		OK		
412	1268			1	http://workforce.tesla.com	workforce.tesla.com		1	e1792.dsc	104.111.216.50		80		OK		
413	115			1	http://www-static-dev.tesla.com	www-static-dev.tesla.com		1	www-static	199.66.9.47		80		OK		
414	199			1	http://www-static-prod.tesla.com	www-static-prod.tesla.com		1	www-static	199.66.9.47		80		OK		
415	204			1	http://www-static-qa.tesla.com	www-static-qa.tesla.com		1	www-static	199.66.9.47		80		OK		
416	278			1	http://www-static-stage.tesla.com	www-static-stage.tesla.com		1	www-static	199.66.9.47		80		OK		
417	290			1	http://www-test.tesla.com	www-test.tesla.com		1	www-test	123.217.138.108,23.202.231.167		80		OK		
418	807			1	http://www-uat-qa.tesla.com	www-uat-qa.tesla.com		1	www-uat	199.66.9.47		80		OK		
419	126			1	http://www-uat.tesla.com	www-uat.tesla.com		1	www-uat	199.66.9.47		80		OK		
420	132			1	http://www-uat2.tesla.com	www-uat2.tesla.com		1	www-uat2	123.217.138.108,23.202.231.167		80		OK		
421	4			1	http://www.tesla.com	www.tesla.com		1	e1792.dsc	184.27.16.62		80		OK		
422	400			1	http://xapps.tesla.com	xapps.tesla.com		1	xapps.tes	204.74.99.100		80		OK		
423	498			1	http://xmail.tesla.com	xmail.tesla.com		1	xmail.tes	204.74.99.100		80		OK		
424	424			1	http://zta-setup.tesla.com	zta-setup.tesla.com		1	a178.scrip	23.195.82.68		80		OK		

theHarvester



```
1 python theHarvester.py --domain tesla.com --dns-lookup --dns-brute --source
```

<https://github.com/laramies/theHarvester>

版本: v4.2.0 (14 八月 2022)

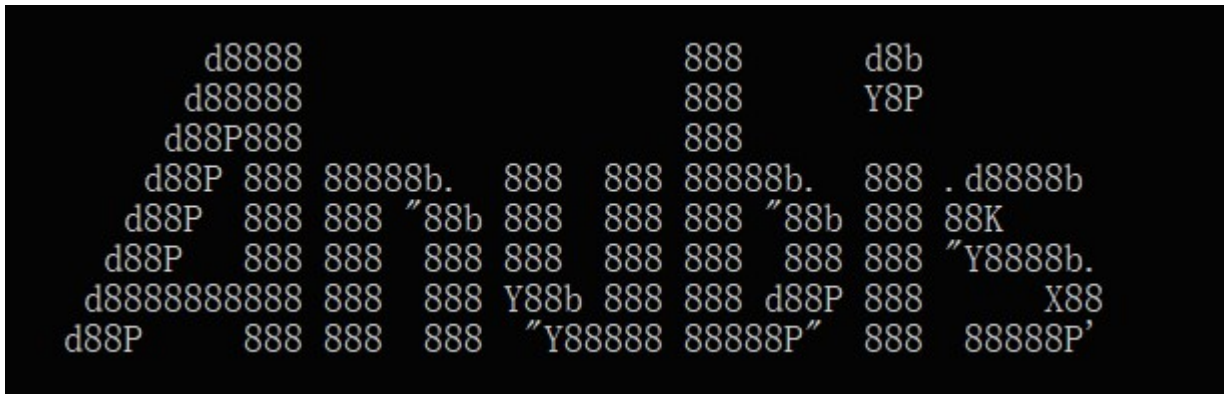
子域: 627

运行时间: 4 分 4 秒

```
*] Hosts found: 1312
-----
0. tesla.com
. tesla.com:3. tesla.com. edgekey.net
. tesla.com:e1792. dscx. akamaiedge.net
. tesla.com:3. tesla.com. edgekey.net.
. tesla.com
7. tesla.com
cademiawashingtonribeiraopreto. tesla.com
cme-sentry-4a. eng. usel. vn. cloud. tesla.com
kamai-apigateway-automation-billing. tesla.com:akamai-apigateway-automation-billing. tesla.com. edgekey.
kamai-apigateway-automation-billing. tesla.com:e1792. dscx. akamaiedge.net
kamai-apigateway-automation. tesla.com:e1792. dscx. akamaiedge.net
kamai-apigateway-automation. tesla.com:akamai-apigateway-automation. tesla.com. edgekey.net
kamai-apigateway-automation. tesla.com:akamai-apigateway-automation. tesla.com. edgekey.net.
kamai-apigateway-automation. tesla.com
kamai-apigateway-bender. tesla.com
kamai-apigateway-bender. tesla.com:e1792. dscx. akamaiedge.net
kamai-apigateway-bender. tesla.com:akamai-apigateway-bender. tesla.com. edgekey.net
kamai-apigateway-bender. tesla.com:akamai-apigateway-bender. tesla.com. edgekey.net.
kamai-apigateway-captiveunderwriting. tesla.com:akamai-apigateway-captiveunderwriting. tesla.com. edgekey.
kamai-apigateway-captiveunderwriting. tesla.com
kamai-apigateway-captiveunderwriting. tesla.com:akamai-apigateway-captiveunderwriting. tesla.com. edgekey.
kamai-apigateway-captiveunderwriting. tesla.com:e1792. dscx. akamaiedge.net
kamai-apigateway-crawford-prd. tesla.com
kamai-apigateway-crawford-prd. tesla.com:e1792. dscx. akamaiedge.net
kamai-apigateway-crawford-prd. tesla.com:akamai-apigateway-crawford-prd. tesla.com. edgekey.net
kamai-apigateway-crawford-stg. tesla.com:e1792. dscx. akamaiedge.net
```

	A	B	C	D	E	F	G	H	I	J	K	L
600	vpn2.tesla.com											
601	vpn3.tesla.com											
602	w3-akamai-apigateway-procuretopayapi.tesla.com											
603	warehouse-stg.tesla.com											
604	warehouse.tesla.com											
605	warpbilling.tesla.com											
606	wdm.kronos.tesla.com											
607	webmail.tesla.com											
608	wim.kronos.tesla.com											
609	workforce.tesla.com											
610	ww.tesla.com											
611	www-dev.tesla.com											
612	www-static-dev.tesla.com											
613	www-static-prod.tesla.com											
614	www-static-qa.tesla.com											
615	www-static-stage.tesla.com											
616	www-stg2.tesla.com											
617	www-test.tesla.com											
618	www-uat-qa.tesla.com											
619	www-uat.tesla.com											
620	www-uat2.tesla.com											
621	www.ug.tesla.com											
622	www45.tesla.com											
623	wwwmta3-emailjenkins.emails.tesla.com											
624	wy7vtk2lup.tesla.com											
625	xapps.tesla.com											
626	mail.tesla.com											
627	zta-setup.tesla.com											
1605												

## Anubis



```
1 anubis -t tesla.com
```

<https://github.com/jonluca/Anubis>

版本: v1.1.3 (10 一月 2023)

子域: 536

运行时间: 31 秒

```
tesla.com
akamai-apigateway-mfs-gfb-stg.tesla.com
referral.tesla.com
akamai-apigateway-vehicleextinfogw-prdsvc-st.tesla.com
origin-www-auth.tesla.com
nuget.github.tesla.com
akamai-apigateway-stg-einvoicing.tesla.com
tcc-graph-stg.tesla.com
lyncdiscover.tesla.com
akamai-apigateway-stg-warpdashboardapi.tesla.com
tcc-gw.tesla.com
o3.ptrl444.tesla.com
darkfield.tesla.com
em7799.tesla.com
integration.kronos.tesla.com
uploads.github.tesla.com
mfa.tesla.com
checkout-ui-assets.tesla.com
monitoring.tesla.com
gridlogic.powerhub.energy.tesla.com
eaa-setup.tesla.com
wwwmta3-emailbjenkins.emails.tesla.com
origin-itanswers.tesla.com
static.tesla.com
events.tesla.com
www-stg2.tesla.com
Sending to AnubisDB
Subdomain search took 0:00:31.547
```

双击可显示空白

amass



```
1 amass enum -passive -d tesla.com -src
```

<https://github.com/OWASP/Amass>

版本: v3.22.2 (21 三月 2023)

子域: 692

运行时间: 4 分 36 秒

---

**开始** **分割** **00:04:36.481** **清除**

**1 停止: 00:04:36.481**

```
RapidDNS] assets.engage.tesla.com
RapidDNS] akamai-apigateway-automation-billing.tesla.com
RapidDNS] origin-pay.tesla.com
RapidDNS] origin-static-assets-teslaaccount.tesla.com
RapidDNS] auth-stage.tesla.com
RapidDNS] teslacdpna03.tesla.com
RapidDNS] origin-bolt-forms.tesla.com
RapidDNS] suppliers-stg.tesla.com
RapidDNS] origin-cicerone.tesla.com
RapidDNS] origin-ownership-web.tesla.com
RapidDNS] origin-trade Partnertickets.tesla.com
RapidDNS] origin-finops.tesla.com
RapidDNS] origin-suppliers.tesla.com
RapidDNS] origin-service.tesla.com
RapidDNS] www-uat-qa.tesla.com
RapidDNS] origin-livestream.tesla.com
RapidDNS] bolt-forms.tesla.com
RapidDNS] origin-suppliers-stg.tesla.com
RapidDNS] teslacdpna04.tesla.com
RapidDNS] teslacdpna05.tesla.com
RapidDNS] stage-uat.tesla.com
RapidDNS] origin-static-assets-pay.tesla.com
RapidDNS] origin-location-services-prd.tesla.com
RapidDNS] origin-warp-akamai.tesla.com
RapidDNS] origin-sales-prd.tesla.com
RapidDNS] origin-partners.tesla.com
RapidDNS] teslacdpna02.tesla.com
RapidDNS] stage-uat-qa.tesla.com
RapidDNS] origin-static-assets-profile-settings.tesla.com
```

## Bbot





```
1 bbot -t tesla.com -f subdomain-enum -c modules.massdns.max_resolvers=5000
```

<https://github.com/blacklanternsecurity/bbot>

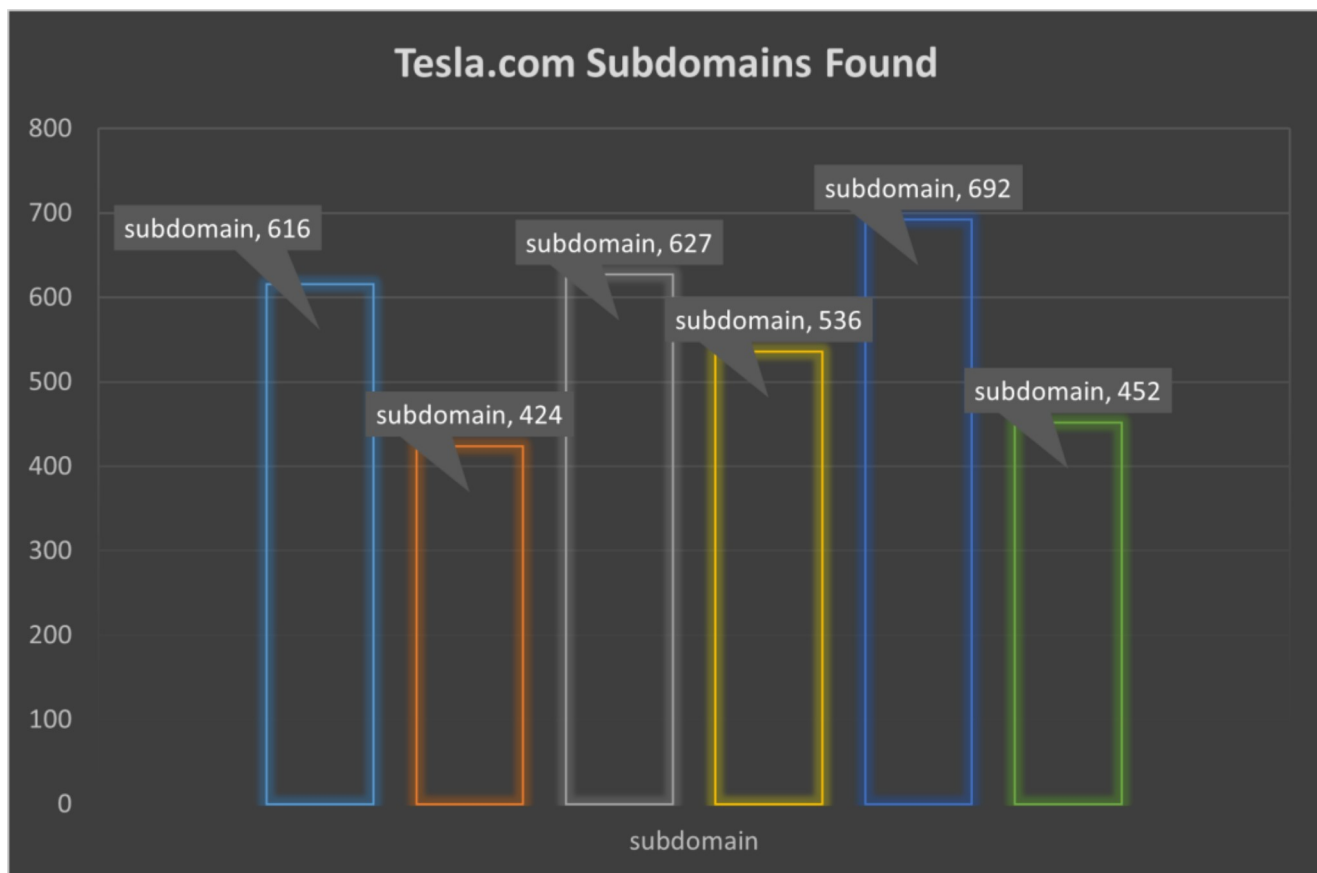
版本: v1.0.5.1331 (10 三月 2023)

子域: 452

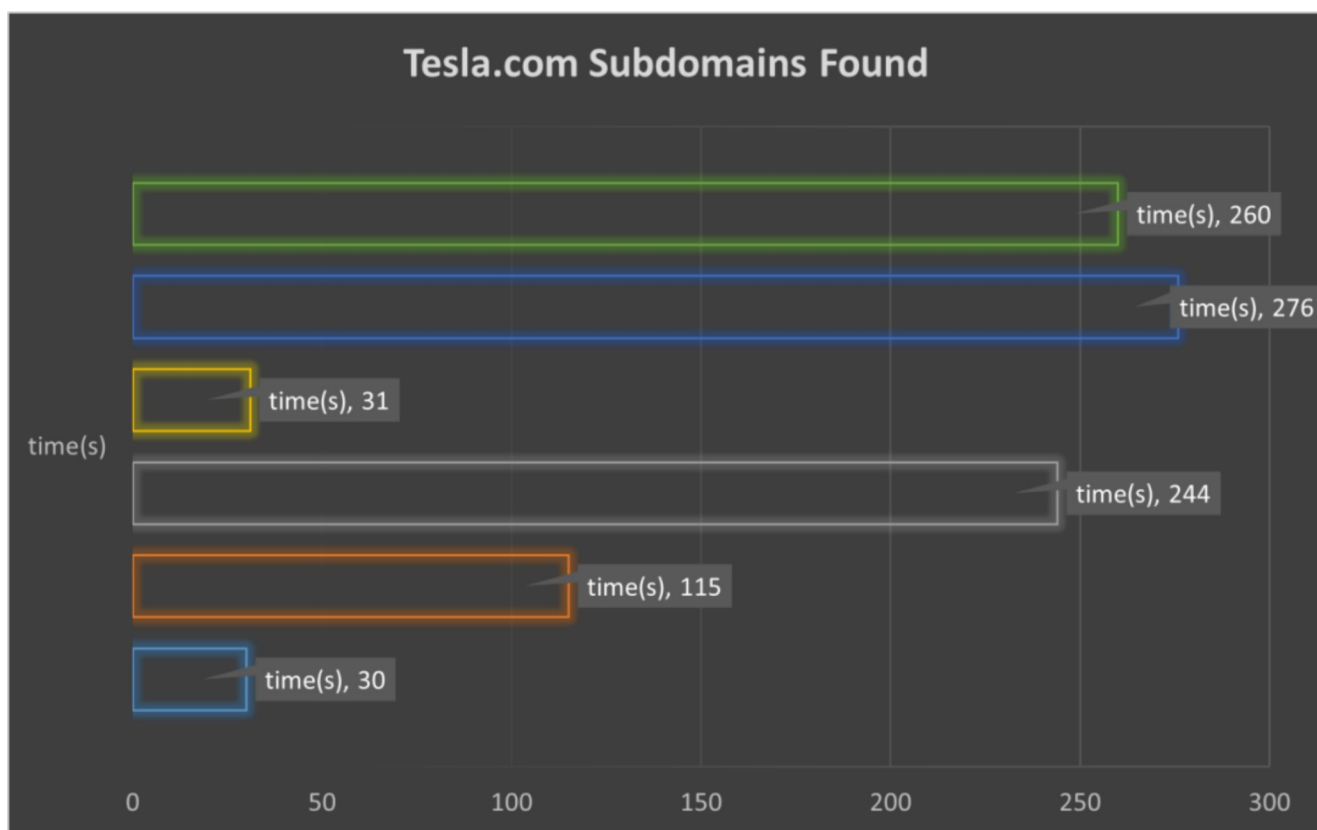
运行时间: 6 分 20 秒

Subdomain	Source
<code>_sip._tls.tesla.com</code>	dnscommonsrv module
<code>_sipfederationtls._tcp.tesla.com</code>	dnscommonsrv module
<code>mta.tesla.com</code>	azure_tenant module
<code>t.tesla.com</code>	azure_tenant module
<code>factory.de.tesla.com</code>	massdns module
<code>origin-myapps.tesla.com</code>	massdns module
<code>origin-profile-stg.tesla.com</code>	massdns module
<code>origin-repair-api-stg.tesla.com</code>	massdns module
<code>origin-repair-api.tesla.com</code>	massdns module
<code>origin-serviceapi-stg.tesla.com</code>	massdns module
<code>origin-serviceapi.tesla.com</code>	massdns module
<code>origin-wwwcdn-new.tesla.com</code>	massdns module
<code>www-uat-integration.tesla.com</code>	massdns module

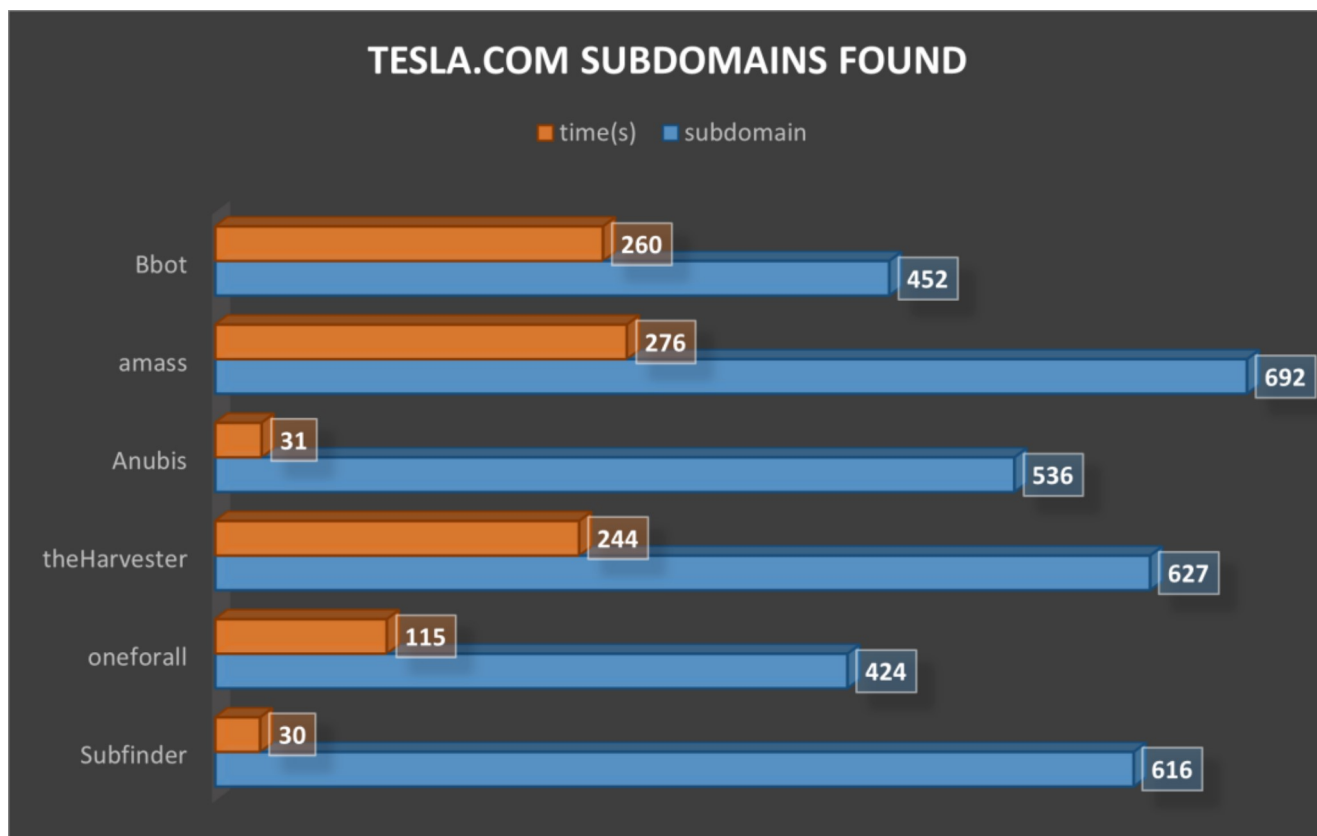
## 六个工具发现的子域名数量结果



## 六个工具发现子域名所用的时间



## 最终结果对比



## 工具主动查找子域名

对于主动爆破子域名，最为重要的是字典，这将在下面会提到。首先我们先来测试一下常用爆破子域名的工具。

测试的工具：

- Fuzzdomain
- Wfuzz
- Gobuster
- Ksubdomain
- Altdns
- Amass

测试规则：

目标: baidu.com

固定使用1300的子域名字典。

在同一台VPS上进行测试, 每个工具单独运行。

## Fuzzdomain

版本: v3.22.2 (21 三月 2023)

子域: 242

运行时间: 1 分 10 秒

开始 分割 **00:01:10.666** 清除

1 停止: 00:01:10.666

The screenshot shows the Fuzzdomain tool interface. At the top, there are controls for domain (baidu.com), level (1), threads (500), and buttons for Start, Browse, Pause, Stop, Stop Browse, Import, and Clear. Below these are checkboxes for dictionary and rule selection. The main area is a table with two columns: Domain and Ip. A red arrow points to the entry '3g.baidu.com'. The status bar at the bottom indicates '开始遍历第1层(当前1/总共1)的3g.baidu.com域名(当前2/总共241)' and '当前35/总共1332'.

Domain	Ip
w.baidu.com	220.181.38.148,220.181.38.251
yq.baidu.com	123.125.115.174,123.125.115.209
gjs.baidu.com	180.97.33.90
md.baidu.com	182.61.62.50
ux.baidu.com	180.76.179.76
tms.baidu.com	182.61.200.85
ub.baidu.com	110.242.69.216
zz.baidu.com	182.61.201.91,182.61.201.90
ep.baidu.com	10.65.211.57
qa.baidu.com	220.181.107.197
sales.baidu.com	49.7.32.140
xf.baidu.com	115.239.210.77
or.baidu.com	39.156.69.32,112.34.111.131
sk.baidu.com	183.232.232.244
gx.baidu.com	180.97.104.235

## Wfuzz

```
1 wfuzz -c -u "http://baidu.com/" -H "Host:FUZZ.baidu.com" -w 1300.txt
```

版本: v3.1.0 (21 六月 2020)

子域: 55

运行时间: 1 分 40 秒

```
000000125: 200      3 L      5 W      81 Ch    "live - live"
000000124: 200      3 L      5 W      81 Ch    "e - e"
000000114: 200      3 L      5 W      81 Ch    "static - static"
000000133: 200      3 L      5 W      81 Ch    "lib - lib"
000000178: 200      3 L      5 W      81 Ch    "mobile - mobile"
000000147: 200      3 L      5 W      81 Ch    "union - union"
000000170: 200      3 L      5 W      81 Ch    "webdisk - webdisk"
000000169: 200      3 L      5 W      81 Ch    "ns2 - ns2"
000000167: 200      3 L      5 W      81 Ch    "pop3 - pop3"
000000166: 200      3 L      5 W      81 Ch    "mx - mx"
000000172: 200      3 L      5 W      81 Ch    "news - news"
000000159: 200      3 L      5 W      81 Ch    "tool - tool"
000000165: 200      3 L      5 W      81 Ch    "webmail - webmail"
000000158: 200      3 L      5 W      81 Ch    "zhidao - zhidao"
000000155: 200      3 L      5 W      81 Ch    "xml - xml"
000000153: 200      3 L      5 W      81 Ch    "edit - edit"
000000154: 200      3 L      5 W      81 Ch    "master - master"
000000150: 200      3 L      5 W      81 Ch    "updates - updates"
000000137: 200      3 L      5 W      81 Ch    "status - status"
000000144: 200      3 L      5 W      81 Ch    "id - id"
000000136: 200      3 L      5 W      81 Ch    "share - share"
000000183: 200      3 L      5 W      81 Ch    "media - media"
000000200: 200      3 L      5 W      81 Ch    "mobilemail - mobilemail"
```

## Gobuster

版本: v3.1.0 (20 二月 2023)

子域: 175

运行时间: 3 分 20 秒

```
1 gobuster dns -d.baidu.com -w 1300.txt
```

```
Found: vv.baidu.com30 (92.86%)
Found: wk.baidu.com30 (93.76%)
Found: xi.baidu.com30 (94.66%)
Found: xr.baidu.com30 (95.79%)
Found: xy.baidu.com
Found: yc.baidu.com30 (96.69%)
Found: yd.baidu.com
Found: yx.baidu.com30 (97.67%)
Found: zc.baidu.com
Found: zn.baidu.com30 (98.72%)
Found: zt.baidu.com
Found: zy.baidu.com30 (99.77%)
Progress: 1330 / 1330 (100.00%)
=====
2023/04/21 16:58:39 Finished
=====
```

## Ksubdomain

版本: v0.7 (12 一月 2021)

子域: 349

运行时间: 32 秒

```
1 ksubdomain-d baidu.com -f 1300.txt
```

```
whois.baidu.com => 180.76.105.190
md.baidu.com => CNAME bapp.n.shifen.com => CNAME domain-offline.baidu.com => 182.61.62.50
cb.baidu.com => CNAME cb.e.shifen.com => 180.101.49.206
local.baidu.com => CNAME shenbian.baidu.com => CNAME shenbian.n.shifen.com
rms.baidu.com => CNAME new.rms.baidu.com
ns6.baidu.com => 111.20.4.13 => 14.215.179.57
its.baidu.com => CNAME api.jt.map.n.shifen.com => 180.97.33.90
mms.baidu.com => CNAME www.baidu.com => CNAME www.a.shifen.com => 180.101.50.188 => 180.101.50.242
red.baidu.com => 10.42.4.86 => 10.26.3.240 => 10.36.4.130 => 10.91.160.44
hybrid.baidu.com => CNAME njsz.api.int.n.shifen.com => 10.207.7.202 => 10.199.6.11
2012.baidu.com => CNAME news.n.shifen.com => 180.101.49.131 => 180.97.33.136
zy.baidu.com => CNAME ziyuan.n.shifen.com => 180.97.104.236 => 180.97.104.55
du.baidu.com => CNAME wap.n.shifen.com => 180.97.34.93 => 180.97.34.91
fq.baidu.com => 10.83.128.103
jz.baidu.com => CNAME sugar.n.shifen.com => 14.215.178.23 => 14.215.178.43
ux.baidu.com => 180.76.179.76
tm.baidu.com => CNAME sftj.e.shifen.com => 180.101.49.100
ut.baidu.com => 10.23.248.87
rq.baidu.com => CNAME huiyan.map.n.shifen.com => 180.97.33.90
u.baidu.com => CNAME u.e.shifen.com => 220.181.111.34
map.baidu.com => CNAME map.n.shifen.com => 180.97.93.90 => 180.97.93.91
education.baidu.com => CNAME open.a.shifen.com => 180.97.33.181 => 180.97.33.183
ee.baidu.com => 10.46.133.175
hr.baidu.com => CNAME talent.baidu.com => 112.34.111.181 => 220.181.111.113 => 111.206.208.251
pda.baidu.com => CNAME wap.n.shifen.com => 180.97.34.91 => 180.97.34.93
partner.baidu.com => 220.181.33.224 => 110.242.68.79 => 112.34.113.34
ke.baidu.com => CNAME wenku.n.shifen.com => 180.101.212.154 => 180.101.212.35
qy.baidu.com => CNAME im.n.shifen.com => 180.101.50.118 => 180.97.34.138
Success:349 Sent:1589 Recved:1330 Faild:0.
```

## Alddns

版本: v1 (2021)

子域: 240

运行时间: 4分32 秒

```
1 altdns -i 1.txt -w 1300.txt -o 2.txt -r -s 11.txt
```

```
n.baidu.com : wap.n.shifen.com.  
mp.baidu.com : gamenew.n.shifen.com.  
es.baidu.com : vr.baidu.com.  
net.baidu.com : 10.242.123.17  
2012.baidu.com : news.n.shifen.com.  
rms.baidu.com : new.rms.baidu.com.  
code.baidu.com : bapp.n.shifen.com.  
ai.baidu.com : ai.n.shifen.com.  
feedback.baidu.com : bapp.n.shifen.com.  
rq.baidu.com : huiyan.map.n.shifen.com.  
pay.baidu.com : dianquan.n.shifen.com.  
gd.baidu.com : 10.57.239.38  
ts.baidu.com : api.jt.map.n.shifen.com.  
job.baidu.com : open.a.shifen.com.  
q.baidu.com : 10.83.128.103  
m.baidu.com : im.n.shifen.com.  
enterprise.baidu.com : tag.baidu.com.  
[*] 500/1330 completed, approx 0:21:51 left  
ms.baidu.com : www.baidu.com.  
sql.baidu.com : sql.e.shifen.com.  
ab.baidu.com : 110.242.69.216  
travel.baidu.com : lvyou.baidu.com.  
feed.baidu.com : wap.n.shifen.com.  
www8.baidu.com : www8.a.shifen.com.  
ms.baidu.com : bce-market.n.shifen.com.  
bd.baidu.com : bd.baidu.com.a.bdydns.com.  
proxy.baidu.com : ns3.baidu.com.  
crm.baidu.com : crm.e.shifen.com.  
p.baidu.com : psdev64.a.shifen.com.  
v.baidu.com : cz-audio.n.shifen.com.
```

## Amass

版本: v3.22.2 (21 三月 2023)

子域: 214

运行时间: 3 分 36 秒

```
1 amass enum -active -brute -d baidu.com -w 1300.txt
```

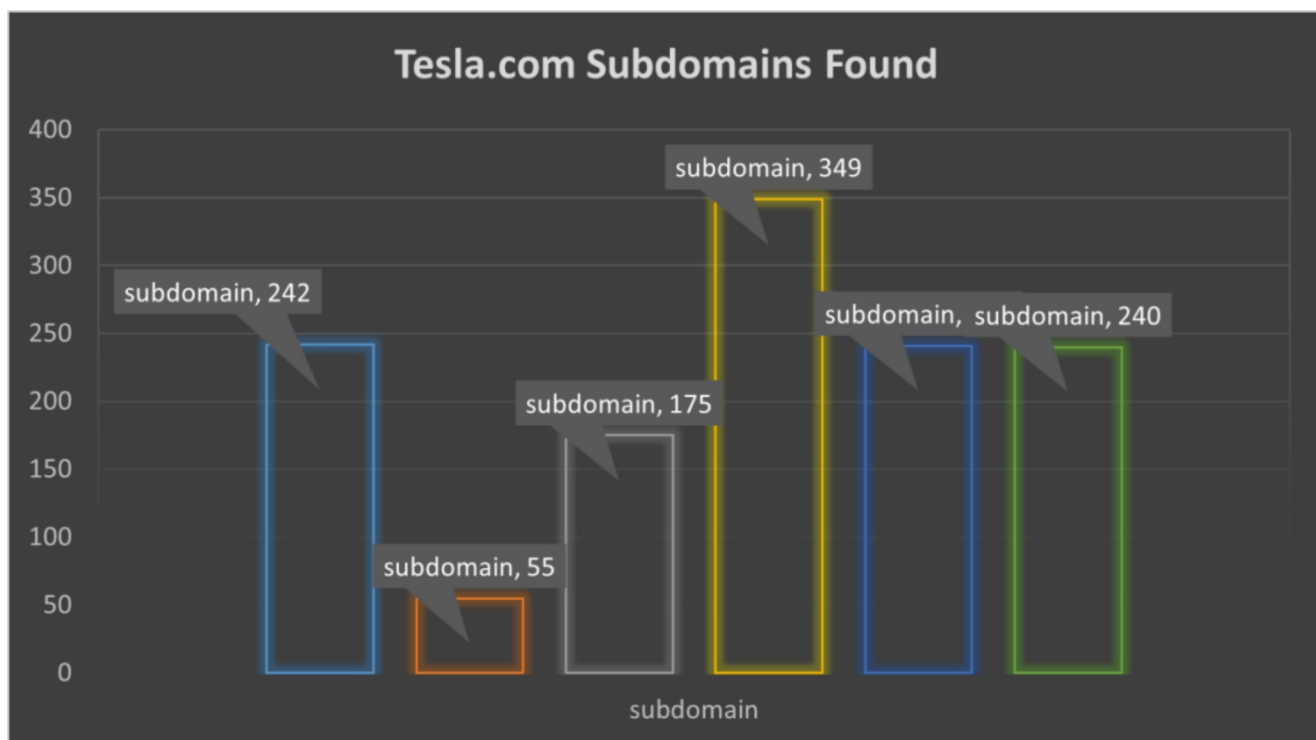


```

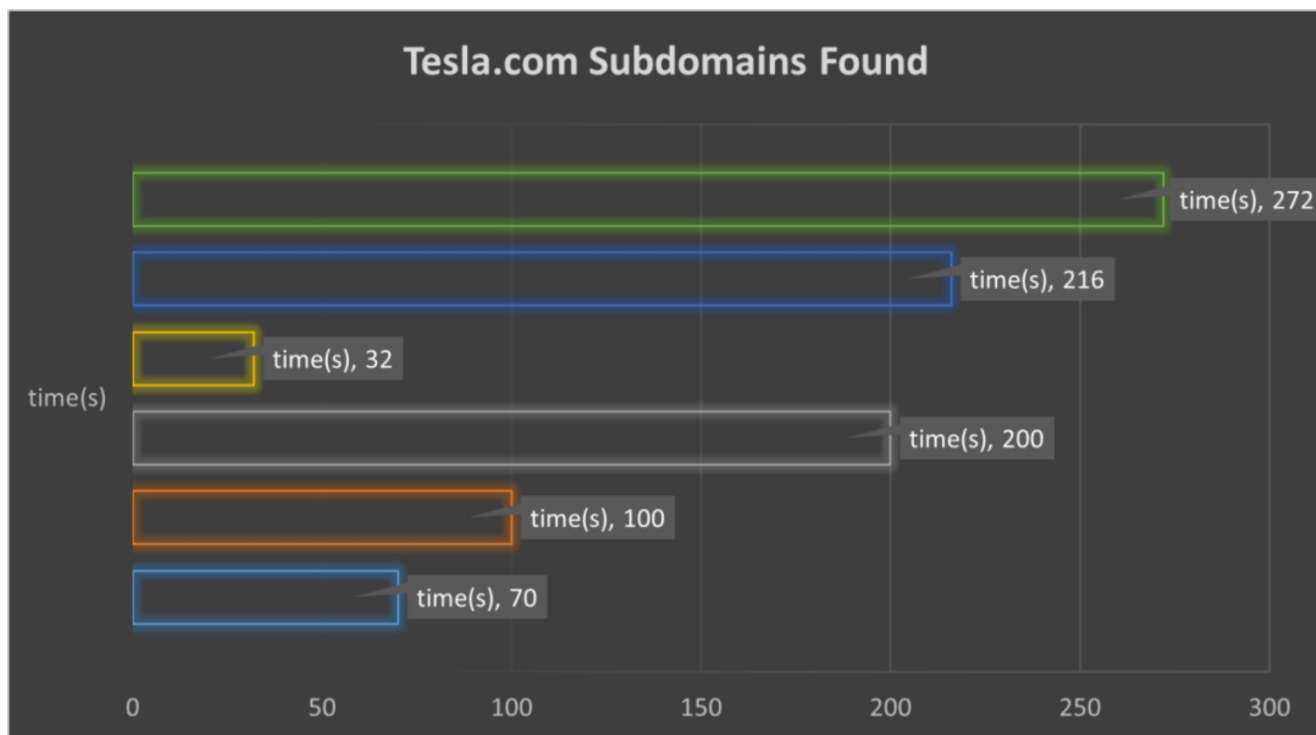
ping.baidu.com
sw.baidu.com
liange.baidu.com
e.dianying.baidu.com
capi.im.baidu.com
edianying.baidu.com
ndianying.baidu.com
qml.baidu.com
movieapp.baidu.com
feeds.baidu.com
in.baidu.com
jifen.baidu.com
ar.mbd.baidu.com
code.baidu.com
duwear.baidu.com
cc.baidu.com
t7.baidu.com
mc.baidu.com
jzapi.baidu.com
v.tieba.baidu.com
funnyjoin.baidu.com
grayline.baidu.com
sipage.bce.baidu.com
iv.baidu.com
mapv.baidu.com
baiduspider-123-125-71-30.crawl.baidu.com
qlb.baidu.com
publish-pic.cpu.baidu.com
yjsstatic.baidu.com
jiaoyu.news.baidu.com
metrics.baidu.com
xiaowu-edge.baidu.com
baiduspider-116-179-32-174.crawl.baidu.com
apollo.baidu.com
ml.mbd.baidu.com
imgnews.baidu.com
iwangmeng.baidu.com
f12.baidu.com
mtj.baidu.com
oos.baidu.com
font-static.baidu.com
i.top.baidu.com
join.baidu.com
ql.baidu.com
static.su.baidu.com
OWASP Amass v3.19.3 https://github.com/OWASP/Amass

```

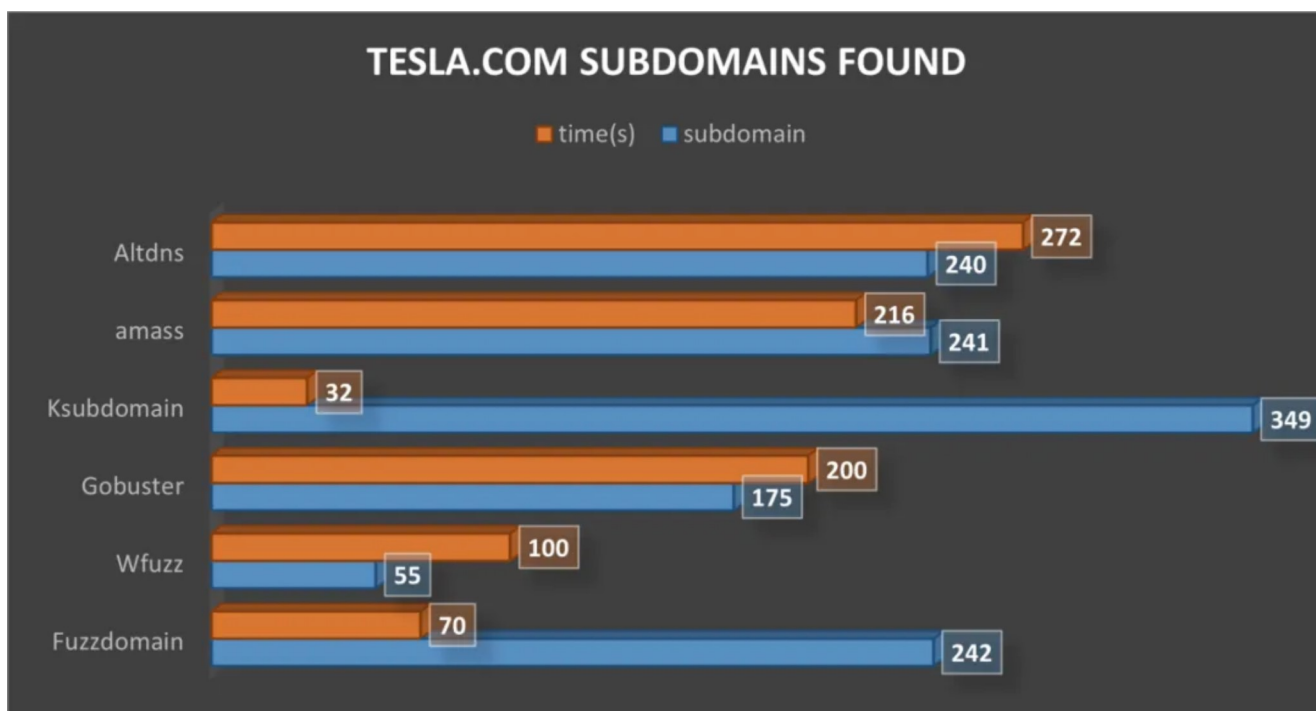
## 六个工具发现的子域名数量结果



## 六个工具发现子域名所用的时间



## 最终结果



## 字典

新子域的开发和部署是动态的，它们会随着时间的推移而变化，我们的字典应该同样动态地反映这一点。为了保持最新状态，我们可以使用惊人的commonspeak2数据集。

<https://github.com/assetnote/wordlists>

可以使用以下命令一次下载所有单词列表：

```
1 wget -r --no-parent -R "index.html*" https://wordlists-cdn.assetnote.io/data
```

字典占用空间达到了接近七个G

	data
类型:	文件夹
位置:	D:\爆破字典
大小:	6.80 GB (7,305,676,341 字节)
占用空间:	6.80 GB (7,307,018,240 字节)
包含:	669 个文件, 4 个文件夹

> "data"中的搜索结果 subdomain

2m-subdomains.txt	D:\爆破字典\dat...	大小: 28.0 MB
修改日期: 2023/3/28 21:14		
httparchive_subdomains_2022_10_28.txt	D:\爆破字典\dat...	大小: 26.3 MB
修改日期: 2023/3/28 21:14		
httparchive_subdomains_2022_12_28.txt	D:\爆破字典\dat...	大小: 32.9 MB
修改日期: 2023/3/28 21:14		
httparchive_subdomains_2023_03_28.txt	D:\爆破字典\dat...	大小: 32.8 MB
修改日期: 2023/3/28 21:14		
httparchive_subdomains_2022_08_28.txt	D:\爆破字典\dat...	大小: 26.9 MB
修改日期: 2023/3/28 21:14		
httparchive_subdomains_2022_09_28.txt	D:\爆破字典\dat...	大小: 24.8 MB
修改日期: 2023/3/28 21:14		
httparchive_subdomains_2022_05_28.txt	D:\爆破字典\dat...	大小: 14.6 MB
修改日期: 2023/3/28 21:14		
httparchive_subdomains_2022_06_28.txt	D:\爆破字典\dat...	大小: 14.1 MB
修改日期: 2023/3/28 21:14		
httparchive_subdomains_2022_07_28.txt	D:\爆破字典\dat...	大小: 18.5 MB
修改日期: 2023/3/28 21:14		
httparchive_subdomains_2021_11_28.txt	D:\爆破字典\dat...	大小: 15.3 MB
修改日期: 2023/3/28 21:14		

## 在线网站

[https://otx.alienvault.com/api/v1/indicators/domain/baidu.com/url\\_list?limit=10000&page=1](https://otx.alienvault.com/api/v1/indicators/domain/baidu.com/url_list?limit=10000&page=1)

```

{
  "url_list": [
    {
      "url": "http://www.baidu.com/home/page/data/pageserver?errno=7004&from=superman&t1682214792367",
      "date": "2023-04-23T00:16:06",
      "domain": "baidu.com",
      "hostname": "www.baidu.com",
      "result": {
        "urlworker": {
          "ip": "104.193.88.77",
          "http_code": 200
        },
        "safebrowsing": {
          "matches": []
        }
      },
      "httpcode": 200,
      "gsb": [],
      "encoded": "http%3A//www.baidu.com/home/page/data/pageserver%3Ferrno%3D7004%26from%3Dsuperman%26_t1682214792367"
    },
    {
      "url": "https://www.baidu.com/link?url=KKC1cZCjagH6HuZPcY3zdEStprM_pk8k1MKXt6_uQIh1Jps1Mrz7hr5",
      "date": "2023-04-22T23:08:46",
      "domain": "baidu.com",
      "hostname": "www.baidu.com",
      "result": {
        "urlworker": {
          "ip": "104.193.88.77",
          "http_code": 404
        },
        "safebrowsing": {
          "matches": []
        }
      },
      "httpcode": 404,
      "gsb": [],
      "encoded": "https%3A//www.baidu.com/link%3Furl%3DKKC1cZCjagH6HuZPcY3zdEStprM_pk8k1MKXt6_uQIh1Jps1Mrz7hr5"
    },
    {
      "url": "http://log.hm.baidu.com/hm.gif?cc=1&ck=1&cl=24-bit&ds=1440x900&ep=2000,100&et=3&ja=1&ln=zh-CN&lo=0&lt=1682207422&nv=0&rnd=1993159134&sl=8245c04923693400737177578c30be1&st=4&v=1.3.0&lv=2",
      "date": "2023-04-22T23:04:39",
      "domain": "baidu.com",
      "hostname": "log.hm.baidu.com",
      "result": {
        "urlworker": {
          "ip": "110.242.68.190",
          "http_code": 200
        },
        "safebrowsing": {
          "matches": []
        }
      }
    }
  ]
}

```

https://quake.360.net

domain:"360.com"

相关ICON (27)

全部展开

经典模式 列表模式

搜索结果 数据统计 聚合分析

开始日期 至 结束日期 导出

hao.360.com EC 中国 北京市 北京市 2023-04-23 08:53:44

443 http/ssl CDN IDC机房 tcp 36.\*\*\*

端口响应 证书 http

hao.360.com

HTTP/1.1 200 OK  
Transfer-Encoding: chunked  
Connection: keep-alive  
Content-Encoding: gzip  
Content-Type: text/html; charset=utf-8  
Date: Sun, 23 Apr 2023 00:49:54 GMT  
Server: nginx

自治域编号	23724	网站服务器	nginx
自治域	China Telecom	网站编程语言	golang
运营商	中国电信	网站路径	/
IP归属	--	主机名	--

https://hunter.qianxin.com

语法检索 domain.suffix="qianxin.com"

最近一个月 全部资产 全部资产标签 +9 全部IP标签 +3 数据去重 否

API 数据导出

序号	资产标签	IP	端口/服务	域名	应用/组件	站点标题	状态码	ICP备案企业
1	WAF	121.32.243.77	443 https	top.gallery.colleg...	奇安信安城	-	200	奇安信科技
2	WAF	121.32.243.77	443 https	docs.mail.college...	奇安信安城	-	200	奇安信科技
3	WAF	121.32.243.77	443 https	bucketcoltano.col...	奇安信安城	-	200	奇安信科技
4	WAF	121.32.243.77	443 https	mail.cloud.colleg...	奇安信安城	-	200	奇安信科技
5	WAF	121.32.243.77	443 https	engine.rd.college...	奇安信安城	-	200	奇安信科技
6	-	120.223.246.95	443 https	dl.qianxin.com	Tengine	-	200	奇安信科技
7	-	211.95.50.152	80 http	sdwan-test.qianxi...	Nginx	奇安信网神安...	200	奇安信科技
8	WAF	223.111.128.84	80 http	amygdala.college...	奇安信安城	-	200	奇安信科技
9	WAF	223.111.128.84	80 http	1bp.college.qianx...	奇安信安城	-	200	奇安信科技
10	WAF	223.111.128.84	80 http	pcprompt-lax.coll...	奇安信安城	-	200	奇安信科技

https://chaziyu.com/tesla.com/



tesla.com

X

查子域名

查备案



**gaopeifu.com**  
**大陆高配服务器**

99元定制服务费



广告



**中介费低至 2.5%**

广告

广告QQ: 3083352837

### tesla.com子域名查询

#### ipchaxun.com

序号	子域名
1	<a href="http://suppliers.tesla.com">suppliers.tesla.com</a>
2	<a href="http://cnvpn1.tesla.com">cnvpn1.tesla.com</a>
3	<a href="http://engage.tesla.com">engage.tesla.com</a>
4	<a href="http://image.emails.tesla.com">image.emails.tesla.com</a>
5	<a href="http://cdn-design.tesla.com">cdn-design.tesla.com</a>
6	<a href="http://trt.tesla.com">trt.tesla.com</a>
7	<a href="http://mobile.tesla.com">mobile.tesla.com</a>

#### chaolianjie.com

序号	子域名
1	<a href="http://www.tesla.com">www.tesla.com</a>
2	<a href="http://tesla.com">tesla.com</a>

https://fofa.info/

FOFA

domain="baidu.com"

🔍

会员 支持及工具

🔔

📄

登录

相关icon(10):

更多 全选

网站指纹排名

all

360,990 条匹配结果 (2,293 条独立IP), 826 ms, 关键词搜索。  
显示一年内数据, 点击 all 查看所有。检测到纯解析域名资产, 点击查看。

☆

↓

API

📄

📊

hDr0q... 256,191

0FC01... 59,794

BzTrDr... 857

UFdiP... 484

OOeq... 288

**https://renwu.baidu.com** 443

[news.n.shifen.com](http://news.n.shifen.com)

14.215.179.120

中国

ASN: 4134

组织: Chinanet

baidu.com

2023-04-23

bfe

HTTP/1.1 500 Internal Server Error

Connection: close

Content-Type: text/plain; charset=utf-8

Date: Sat, 22 Apr 2023 02:58:42 GMT

Server: bfe

Content-Length: 0

国家/地区排名

» 中国 360,695

» 中国香港... 155

» 美国 54

» 日本 25

» 德国 17

+ Certificate 29d21...

https://developers.facebook.com/tools/ct?step\_size=30&query=baidu.com

Meta for Developers 文档 工具 支持 搜索 搜索开发者文档

### 证书透明度监控

证书透明度 是一个开放体系，专门记录、审核并监控在互联网公开受信任的 TLS 证书。通过这个工具，你可以搜索为特定域名签发的证书，并订阅有关新证书签发和潜在钓鱼攻击的 Facebook 通知。

Search Subscriptions

baidu.com 搜索

域	主题	签发者	有效期	证书
otacdn.baidu.com	CN=otacdn.baidu.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust TLS RSA CA G1	Apr 18, 2023 - May 09, 2024	<a href="#">显示详情</a> (CT Precertificate)
app.ka.baidu.com	CN=app.ka.baidu.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1	Apr 17, 2023 - Apr 18, 2024	<a href="#">显示详情</a> (CT Precertificate)
otacdn.baidu.com sni.cloudflaressl.com	C=US, ST=California, L=San Francisco, O=Cloudflare, Inc., CN=sni.cloudflaressl.com	C=US, O=Cloudflare, Inc., CN=Cloudflare Inc RSA CA-2	Apr 17, 2023 - Apr 16, 2024	<a href="#">显示详情</a> (CT Precertificate)
otacdn.baidu.com sni.cloudflaressl.com	C=US, ST=California, L=San Francisco, O=Cloudflare, Inc., CN=sni.cloudflaressl.com	C=US, O=Cloudflare, Inc., CN=Cloudflare Inc ECC CA-3	Apr 17, 2023 - Apr 16, 2024	<a href="#">显示详情</a> (CT Precertificate)
creation.ai.baidu.com inflow.baidu.com bceidaas.com creatore.baidu.com	C=CN, ST=北京, L=北京, O=百度, CN=百度			

https://crt.sh/?q=baidu.com

crt.sh Identity Search 搜索 按颁发者分组

Criteria Type: Identity Match: ILIKE Search: 'baidu.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	9185521173	2023-04-19	2023-04-19	2024-05-09	otacdn.baidu.com	otacdn.baidu.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust TLS RSA CA G1
	9180282638	2023-04-18	2023-04-18	2024-04-16	sni.cloudflaressl.com	otacdn.baidu.com	C=US, O=Cloudflare, Inc., CN=Cloudflare Inc ECC CA-3
	9180282643	2023-04-18	2023-04-18	2024-04-16	sni.cloudflaressl.com	otacdn.baidu.com	C=US, O=Cloudflare, Inc., CN=Cloudflare Inc RSA CA-2
	9178222562	2023-04-18	2023-04-18	2024-04-18	app.ka.baidu.com	app.ka.baidu.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1
	9145175566	2023-04-14	2023-04-14	2024-05-14	misc.baidu.com	abot.pos.baidu.com creation.ai.baidu.com dwz.hm.baidu.com misc.baidu.com *smartapps.baidu.com	C=US, O=DigiCert Inc, CN=DigiCert Secure Site Pro CN CA G3
	9113770139	2023-04-11	2023-04-11	2024-04-30	*.now.baidu.com	*.now.baidu.com	C=US, O=DigiCert Inc, CN=DigiCert Secure Site Pro CN CA G3
	9110779492	2023-04-10	2023-04-10	2024-04-09	*.com-baidu.com	*.com-baidu.com com-baidu.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA
	9110779573	2023-04-10	2023-04-10	2024-04-09	*.com-baidu.com	*.com-baidu.com com-baidu.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA
	9125349733	2023-04-10	2023-04-10	2023-07-09	*.com-baidu.com	*.com-baidu.com com-baidu.com	C=US, O=Let's Encrypt, CN=E1
	9107764799	2023-04-10	2023-04-10	2023-07-09	*.com-baidu.com	*.com-baidu.com com-baidu.com	C=US, O=Let's Encrypt, CN=E1
	9106320623	2023-04-10	2023-04-10	2024-04-09	sni.cloudflaressl.com	*.com-baidu.com com-baidu.com	C=US, O=Cloudflare, Inc., CN=Cloudflare Inc ECC CA-3
	9083551477	2023-04-07	2023-04-07	2024-04-09	beareditorr.bce.baidu.com	beareditorr.bce.baidu.com	C=US, O=DigiCert Inc, CN=DigiCert Secure Site Pro CN CA G3
	9062639686	2023-04-05	2023-04-05	2024-04-04	sni.cloudflaressl.com	otacdn.baidu.com	C=US, O=Cloudflare, Inc., CN=Cloudflare Inc ECC CA-3
	9062640994	2023-04-05	2023-04-05	2024-04-04	sni.cloudflaressl.com	otacdn.baidu.com	C=US, O=Cloudflare, Inc., CN=Cloudflare Inc RSA CA-2
	9045260048	2023-04-03	2023-04-03	2024-04-12	lookup.api.bsb.baidu.com	lookup.api.bsb.baidu.com	C=US, O=DigiCert Inc, CN=DigiCert Secure Site Pro CN CA G3
	9045241968	2023-04-03	2023-04-03	2024-04-11	download.api.bsb.baidu.com	download.api.bsb.baidu.com	C=US, O=DigiCert Inc, CN=DigiCert Secure Site Pro CN CA G3
	9006962018	2023-03-30	2023-03-30	2023-06-28	www.baidu.com	www.baidu.com	C=US, ST=Texas, L=Houston, O=SSL Corporation, CN=SSL.com RSA SSL subCA
	9006755036	2023-03-30	2023-03-30	2024-03-30	mona.bce.baidu.com	mona.bce.baidu.com	C=US, O=DigiCert Inc, CN=DigiCert Secure Site Pro CN CA G3
	9006755536	2023-03-30	2023-03-30	2024-03-30	biior.bce.baidu.com	biior.bce.baidu.com	C=US, O=DigiCert Inc, CN=DigiCert Secure Site Pro CN CA G3
	8983409151	2023-03-27	2023-03-27	2024-04-16	edisk.cloud.baidu.com	edisk.cloud.baidu.com	C=US, O=DigiCert Inc, CN=DigiCert Secure Site Pro CN CA G3
	8998399811	2023-03-27	2023-03-27	2023-06-25	dula.bceitest.baidu.com	dula.bceitest.baidu.com	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	8998399587	2023-03-27	2023-03-27	2023-06-25	dula.bceitest.baidu.com	dula.bceitest.baidu.com	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	8980303317	2023-03-26	2022-07-05	2023-08-06	baidu.com	*.baidu.com baidu.com *.bce.baidu.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018