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

```
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

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

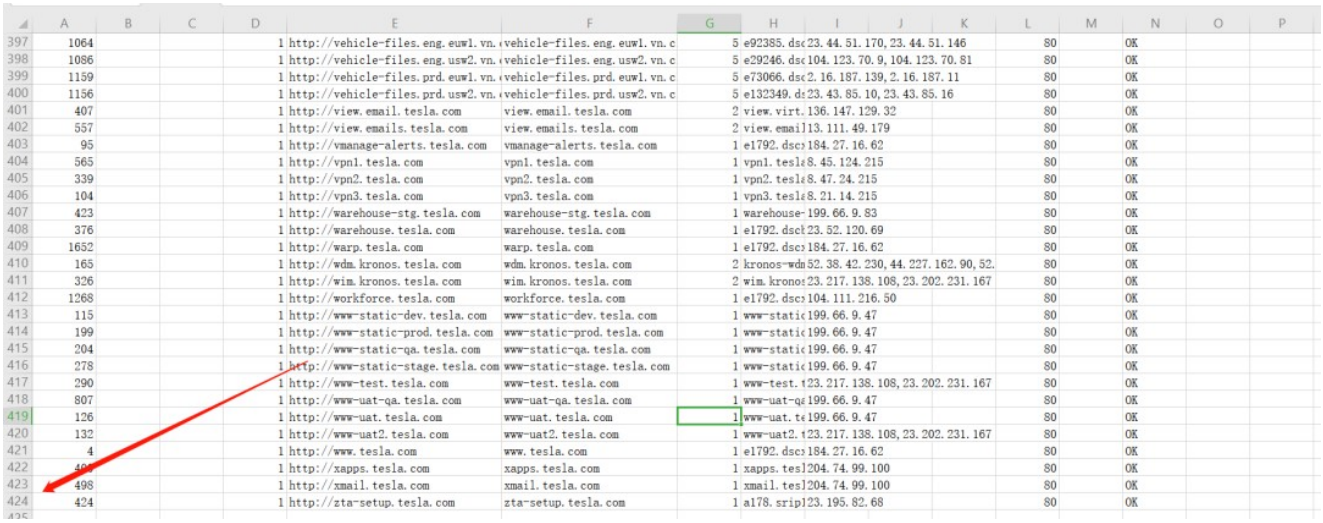
https://github.com/shmilylty/OneForAll

版本：v0.4.5 （10 七月 2022）

子域：424

运行时间：1 分 55 秒


```
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.ds	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	565			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	23.217.138.108, 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.t	23.217.138.108, 23.202.231.167			80		OK		
418	807			1	http://www-uat-qa.tesla.com	www-uat-qa.tesla.com	1	www-uat-qa	199.66.9.47			80		OK		
419	126			1	http://www-uat.tesla.com	www-uat.tesla.com	1	www-uat.te	199.66.9.47			80		OK		
420	132			1	http://www-uat2.tesla.com	www-uat2.tesla.com	1	www-uat2.t	23.217.138.108, 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	499			1	http://xapps.tesla.com	xapps.tesla.com	1	xapps.tesl	204.74.99.100			80		OK		
423	498			1	http://xmail.tesla.com	xmail.tesla.com	1	xmail.tesl	204.74.99.100			80		OK		
424	424			1	http://zta-setup.tesla.com	zta-setup.tesla.com	1	a178.sri	23.195.82.68			80		OK		

theHarvester


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

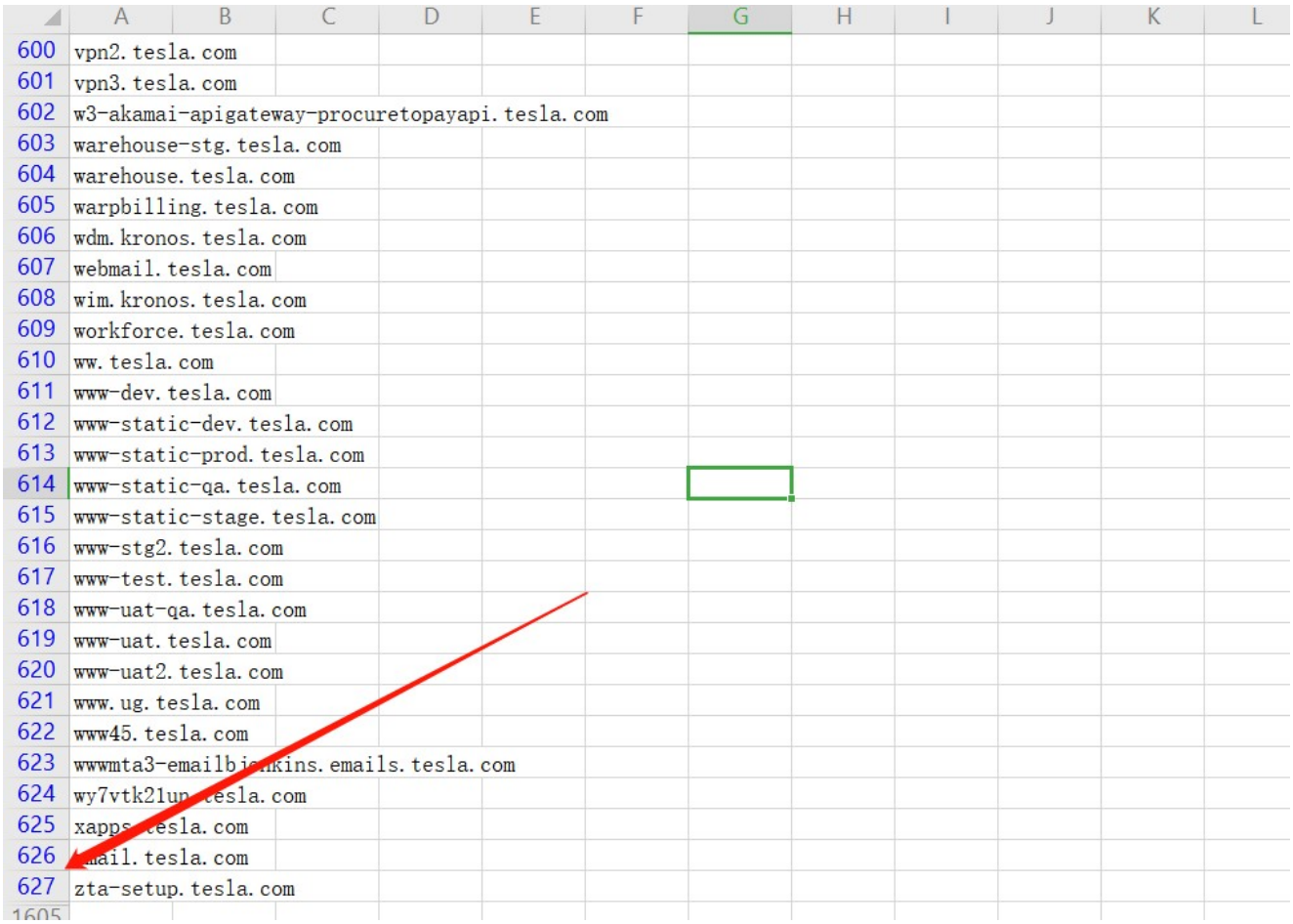
https://github.com/laramies/theHarvester

版本：v4.2.0 （14 八月 2022）

子域：627

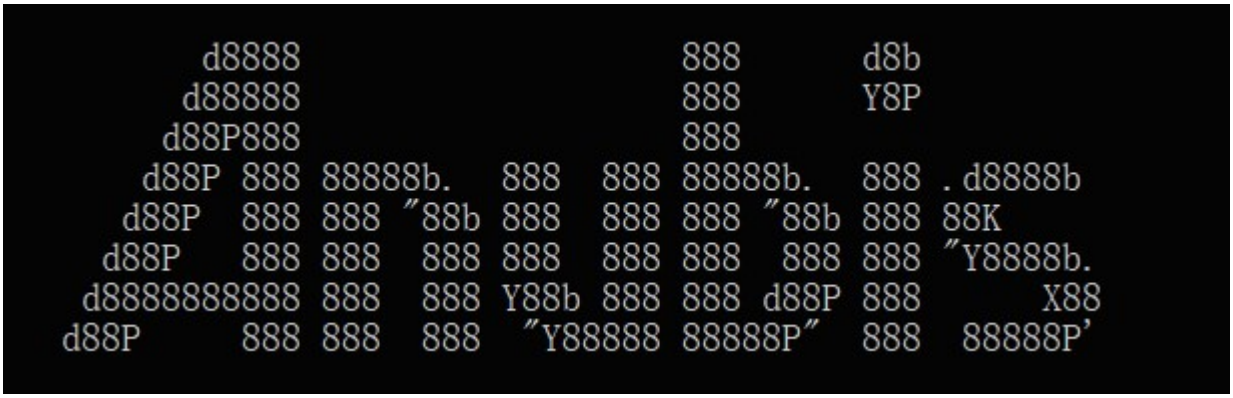
运行时间：4 分 4 秒

```
*] 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.use1.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.edgeke
kamai-apigateway-captiveunderwriting.tesla.com
kamai-apigateway-captiveunderwriting.tesla.com:akamai-apigateway-captiveunderwriting.tesla.com.edgeke
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
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-emailbi[illegible]kins.emails.tesla.com
624	wy7vtk21up[illegible]tesla.com
625	xapps[illegible]tesla.com
626	[illegible]mail.tesla.com
627	zta-setup.tesla.com

Anubis



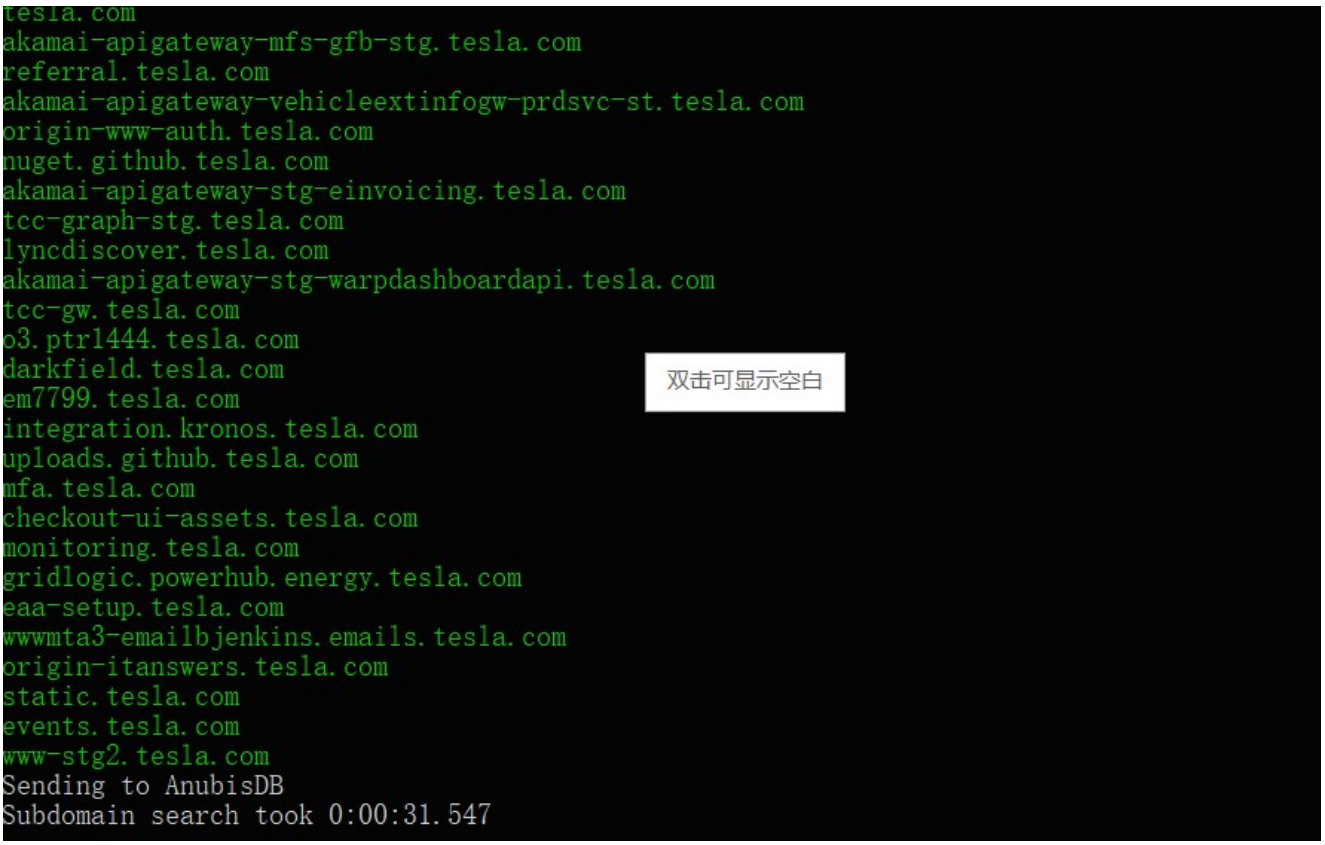

```
anubis -t tesla.com
```

https://github.com/jonluca/Anubis

版本：v1.1.3 （10 一月 2023）

子域：536

运行时间：31 秒



amass


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

https://github.com/OWASP/Amass

版本：v3.22.2 （21 三月 2023）

子域：692

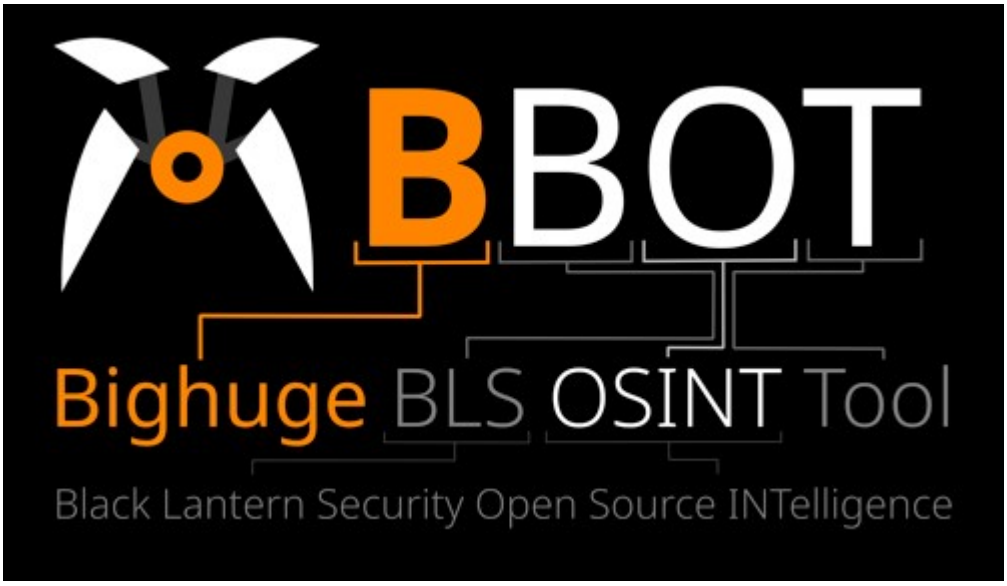
运行时间：4 分 36 秒

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-tradepartnertickets.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



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

https://github.com/blacklanternsecurity/bbot

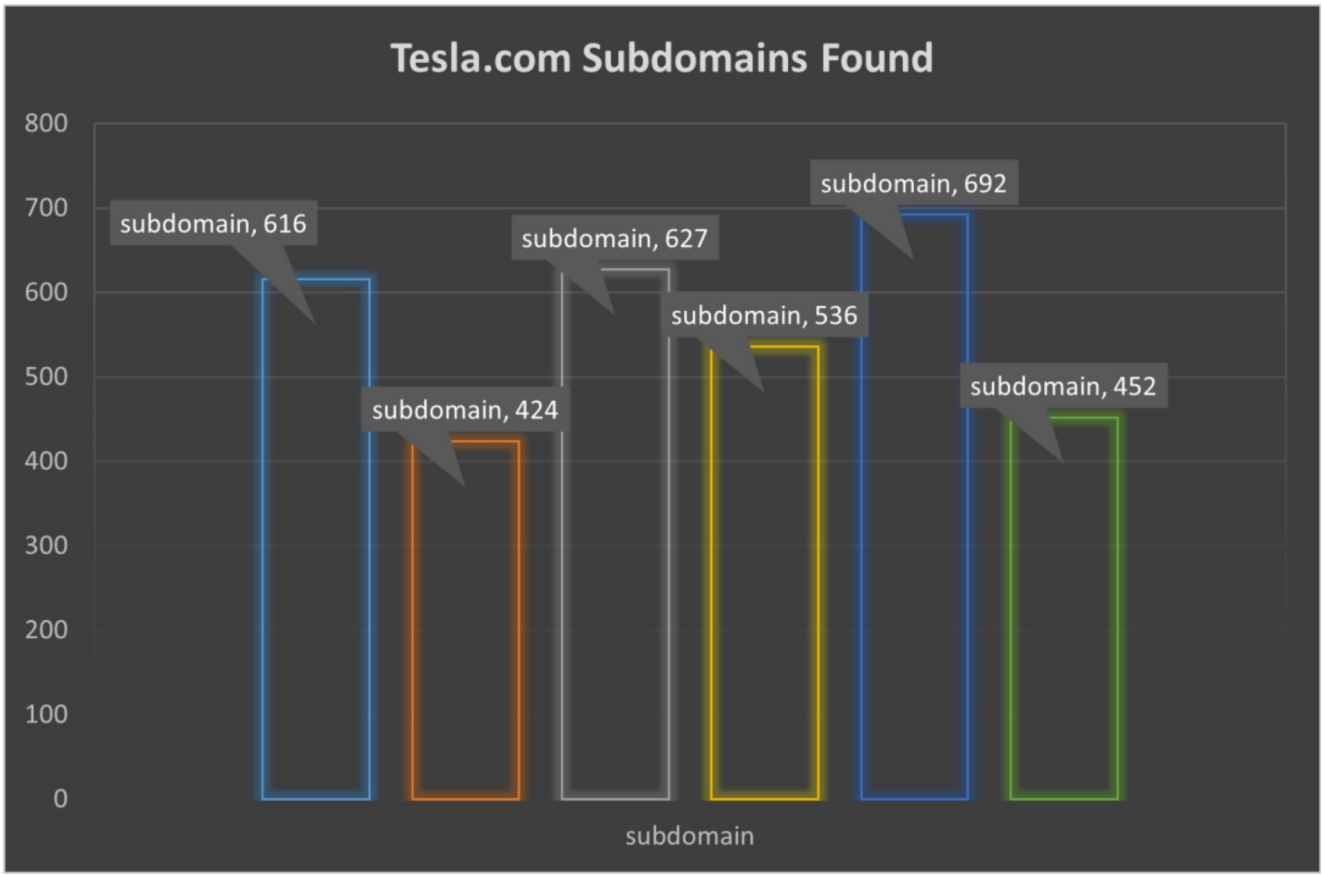
版本：v1.0.5.1331 （10 三月 2023）

子域：452

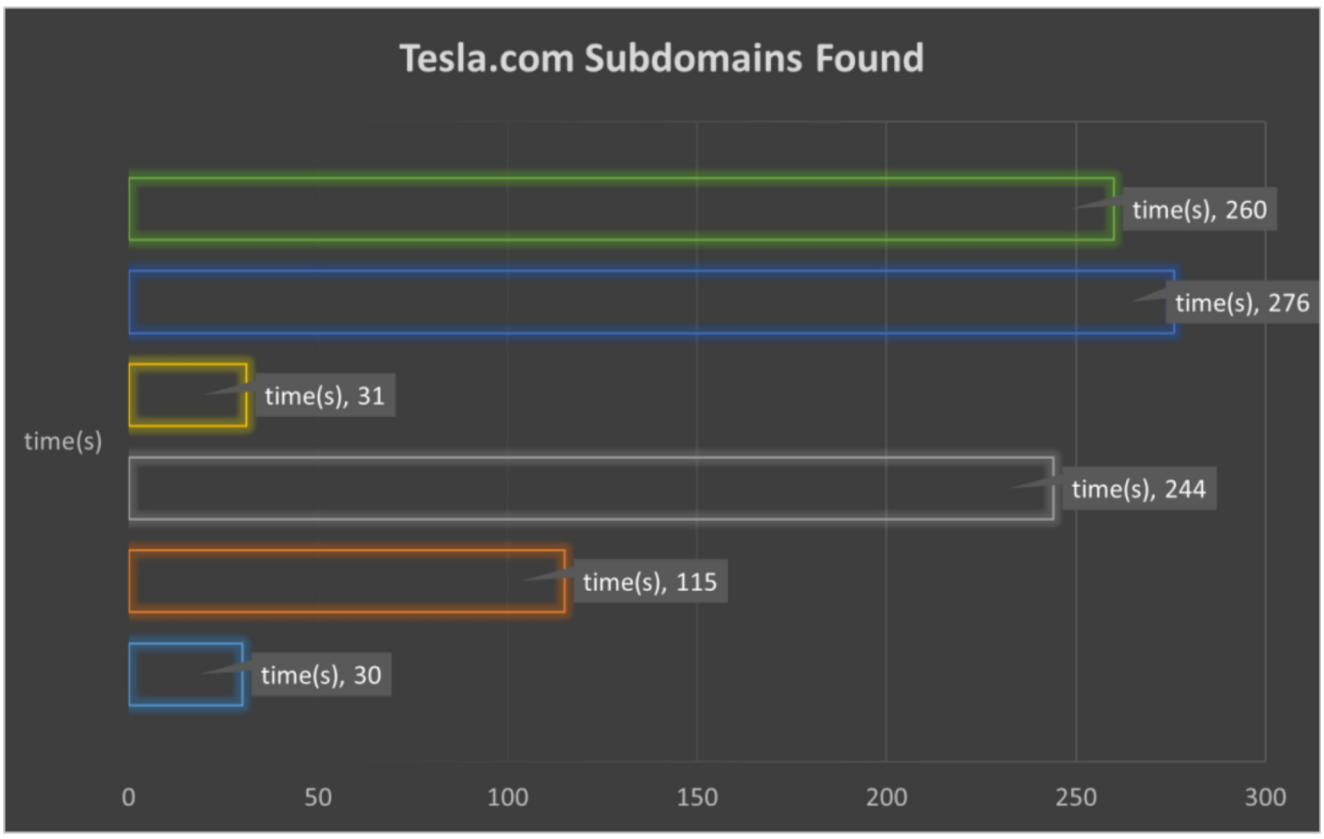
运行时间：6 分 20 秒

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

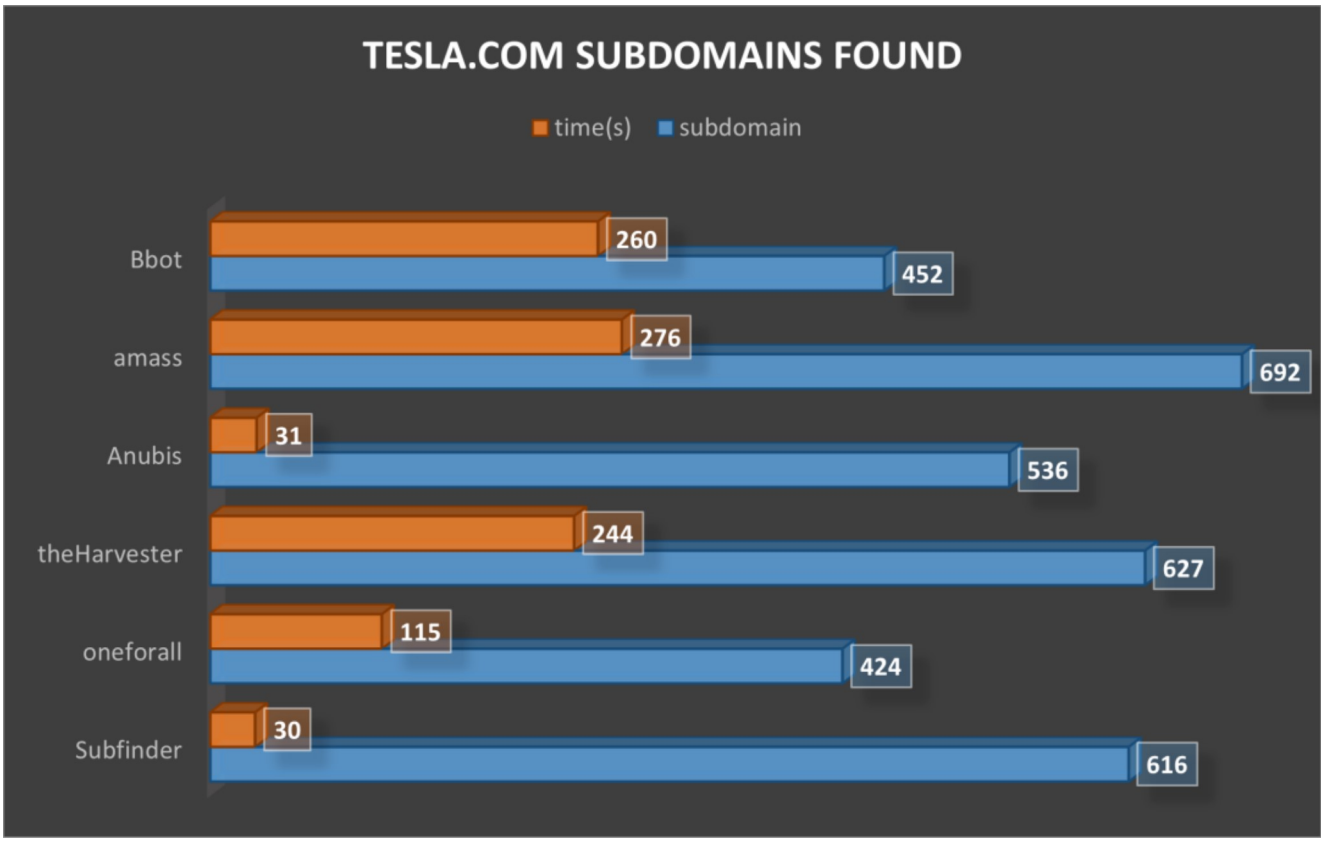
六个工具发现的子域名数量结果



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

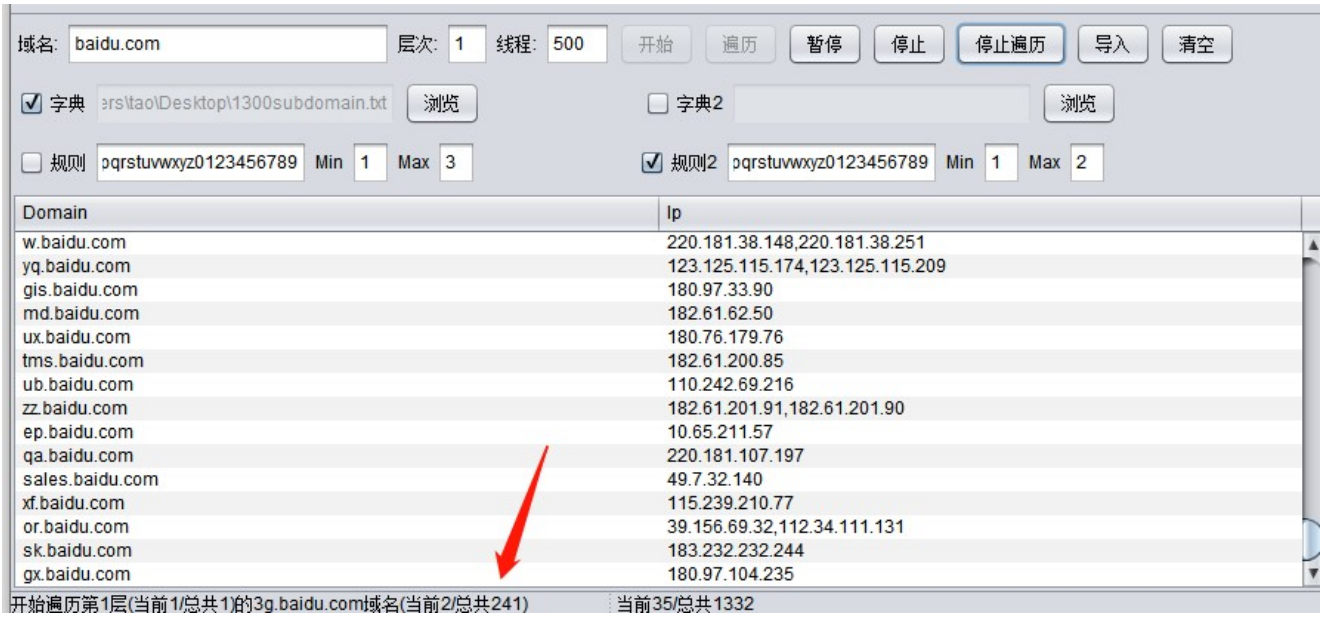
固定使用1300的子域名字典。

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



Wfuzz

```
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"
```

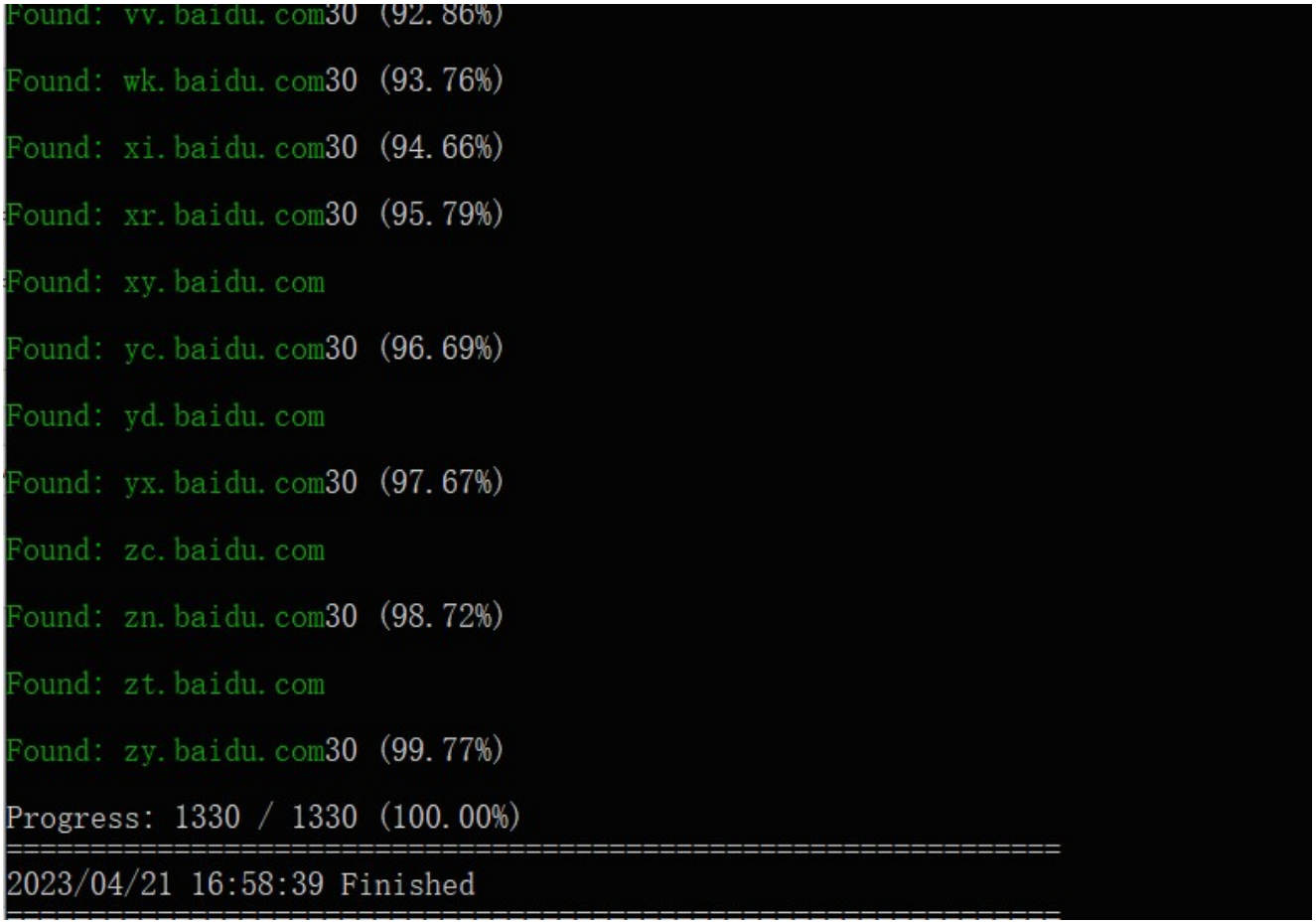
Gobuster

版本：v3.1.0 （20 二月 2023）

子域：175

运行时间：3 分 20 秒

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



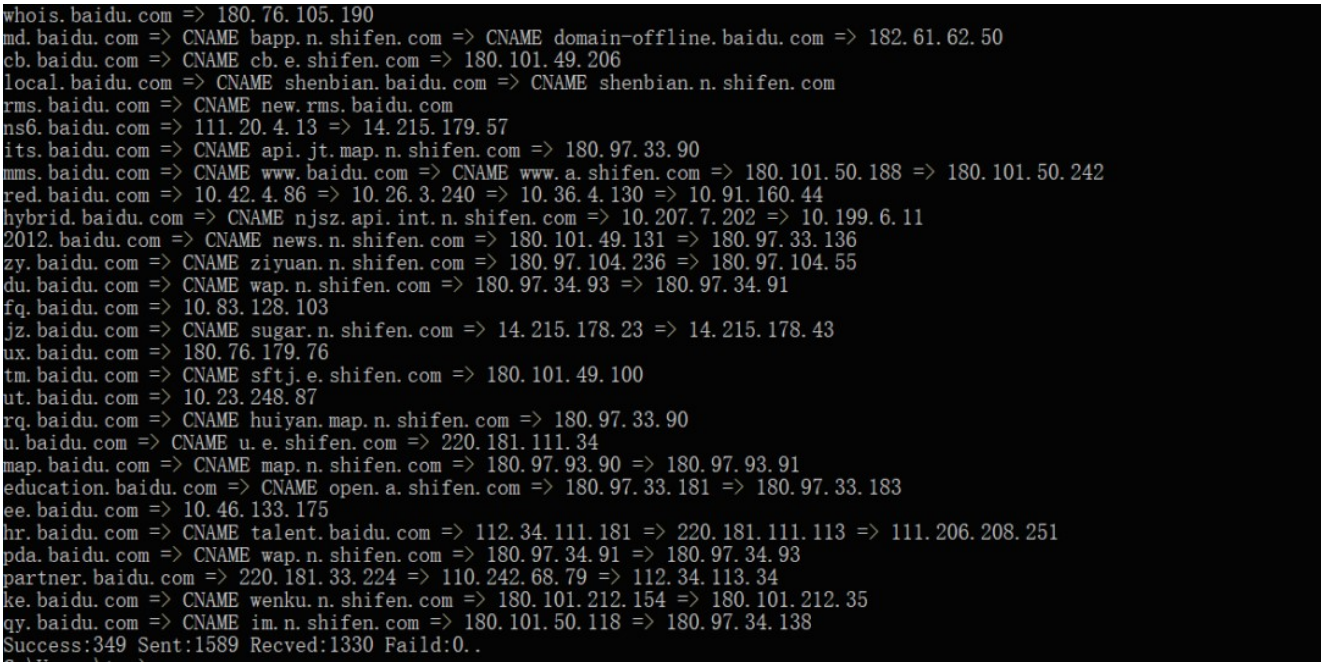
Ksubdomain

版本：v0.7 （12 一月 2021）

子域：349

运行时间：32 秒

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



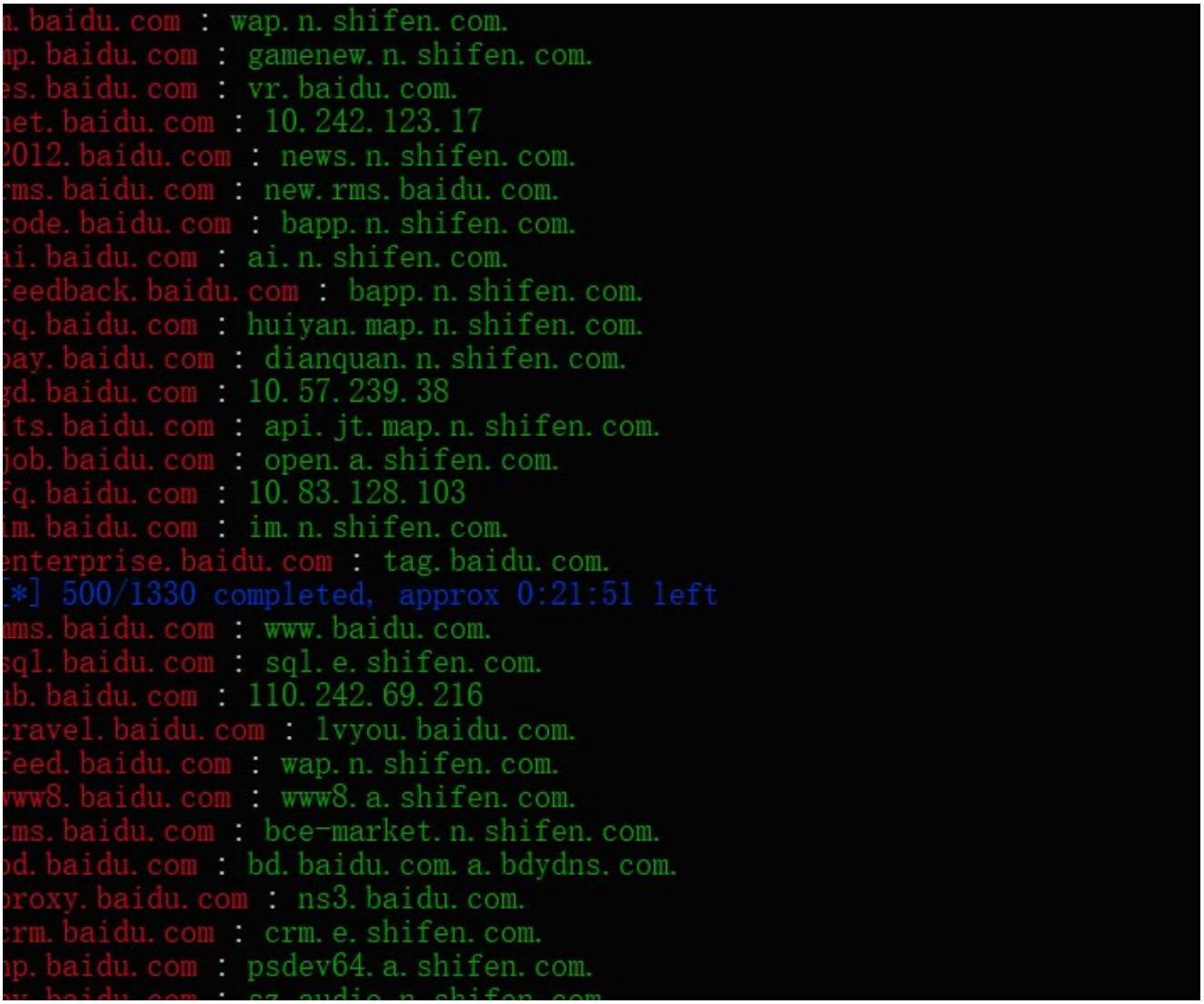
Altdns

版本：v1 （2021）

子域：240

运行时间：4分32 秒

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



Amass

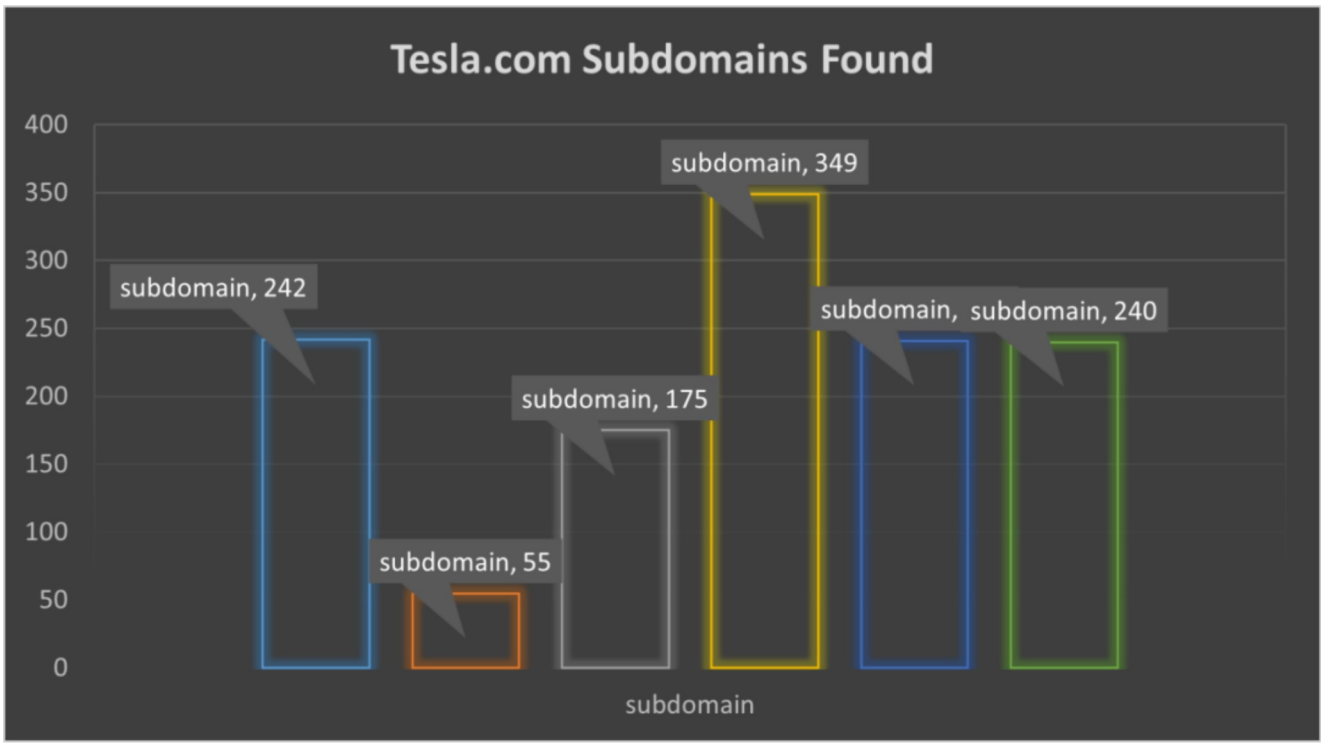
版本：v3.22.2 （21 三月 2023）

子域：214

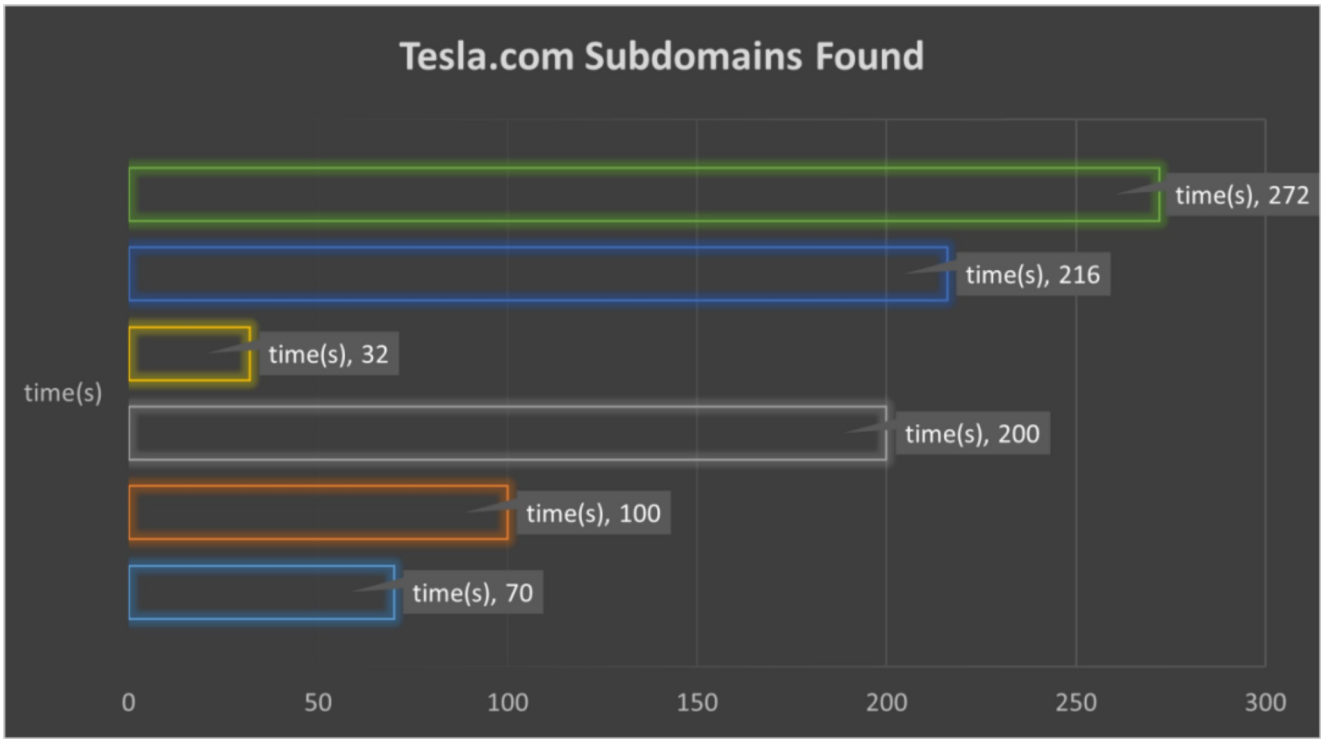
运行时间：3 分 36 秒

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

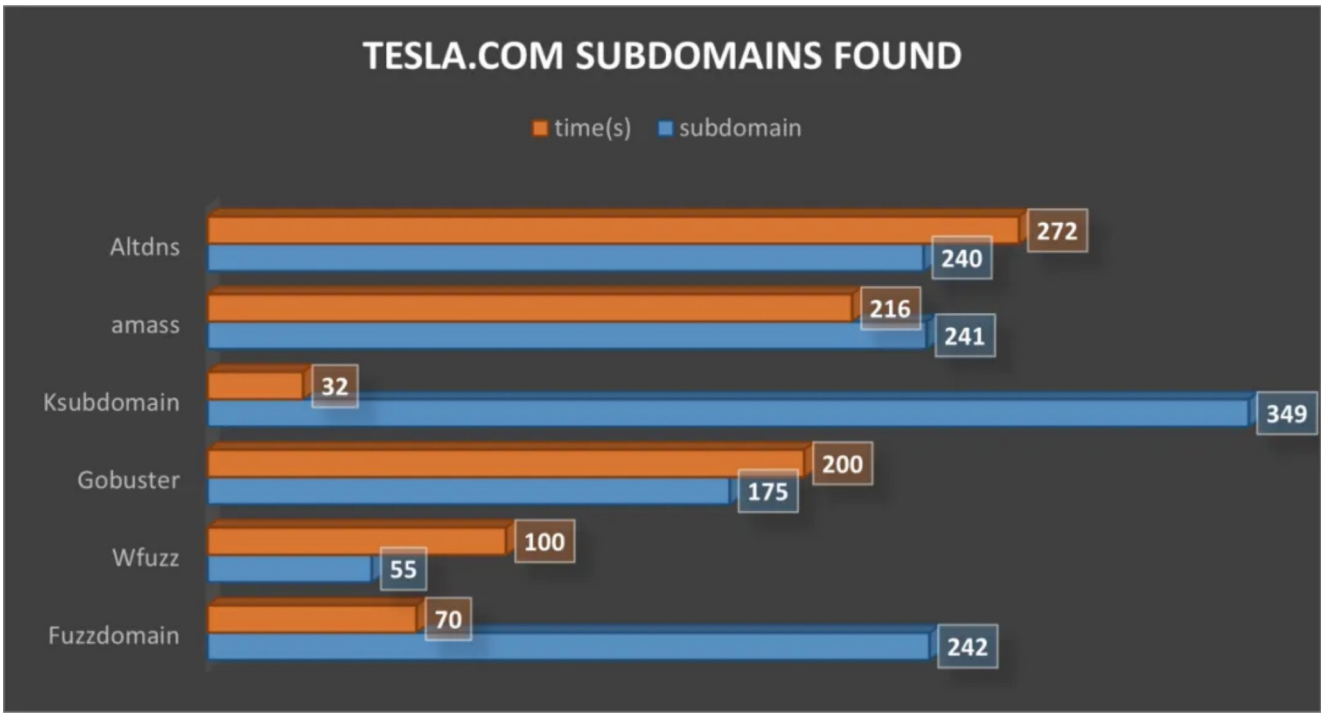
六个工具发现的子域名数量结果



六个工具发现子域名所用的时间


Tesla.com Subdomains Found
time(s)
time(s), 272
time(s), 216
time(s), 32
time(s), 200
time(s), 100
time(s), 70
0
50
100
150
200
250
300

最终结果


TESLA.COM SUBDOMAINS FOUND
time(s)
subdomain
Altdns
272
240
amass
216
241
Ksubdomain
32
349
Gobuster
200
175
Wfuzz
100
55
Fuzzdomain
70
242

字典

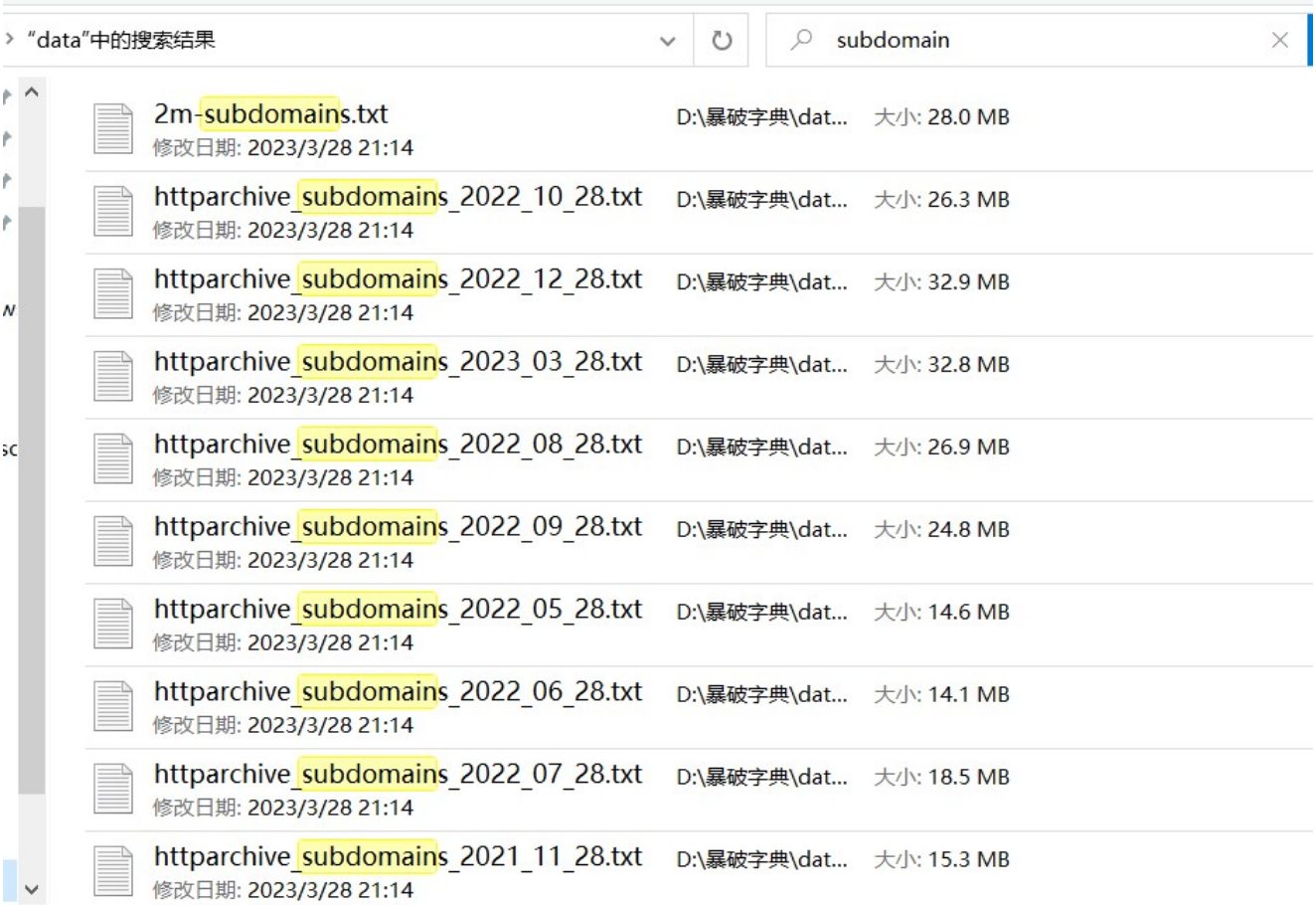
新子域的开发和部署是动态的，它们会随着时间的推移而变化， 我们的字典应该同样动态地反映这一点。为了保持最新状态，我们可以使用惊人的commonspeak2数据集。

https://github.com/assetnote/wordlists

可以使用以下命令一次下载所有单词列表：

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

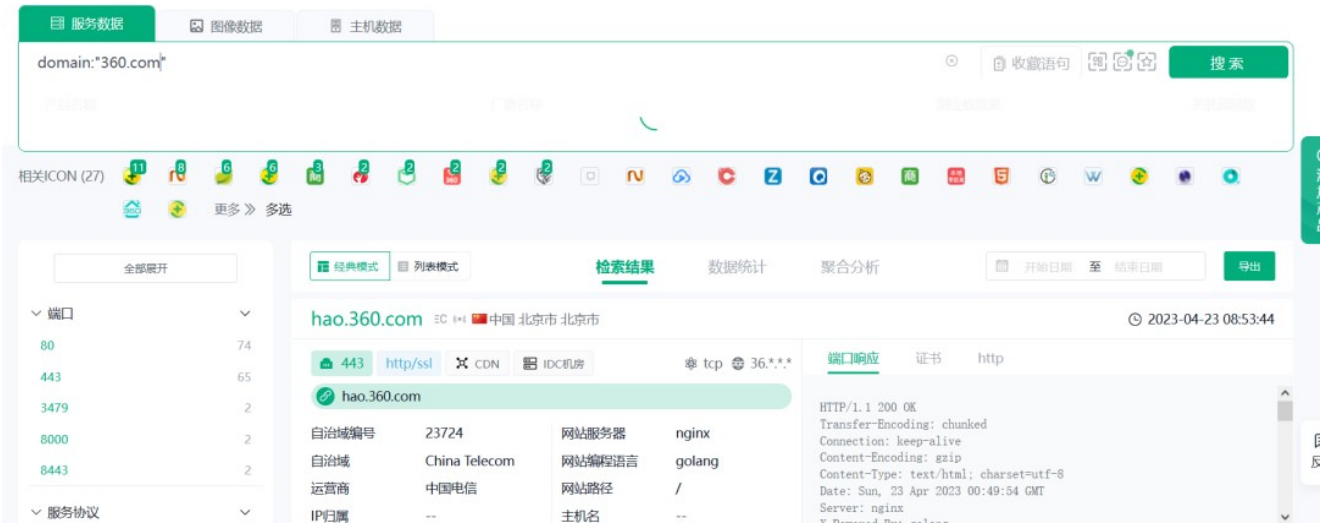
字典占用空间达到了接近七个G



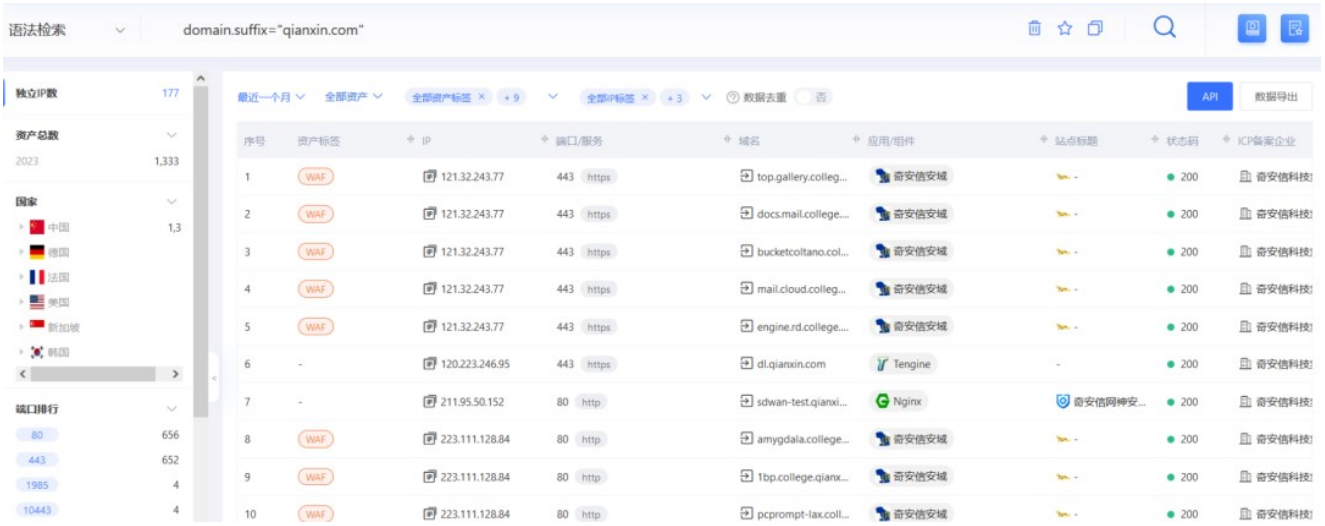
在线网站

https://otx.alienvault.com/api/v1/indicators/domain/baidu.com/url_list?limit=10000&page=1

https://quake.360.net



https://hunter.qianxin.com



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

https://fofa.info/

https://developers.facebook.com/tools/ct?step_size=30&query=baidu.com

Meta for Developers 文档 工具 支持 搜索开发者文档

证书透明度监控

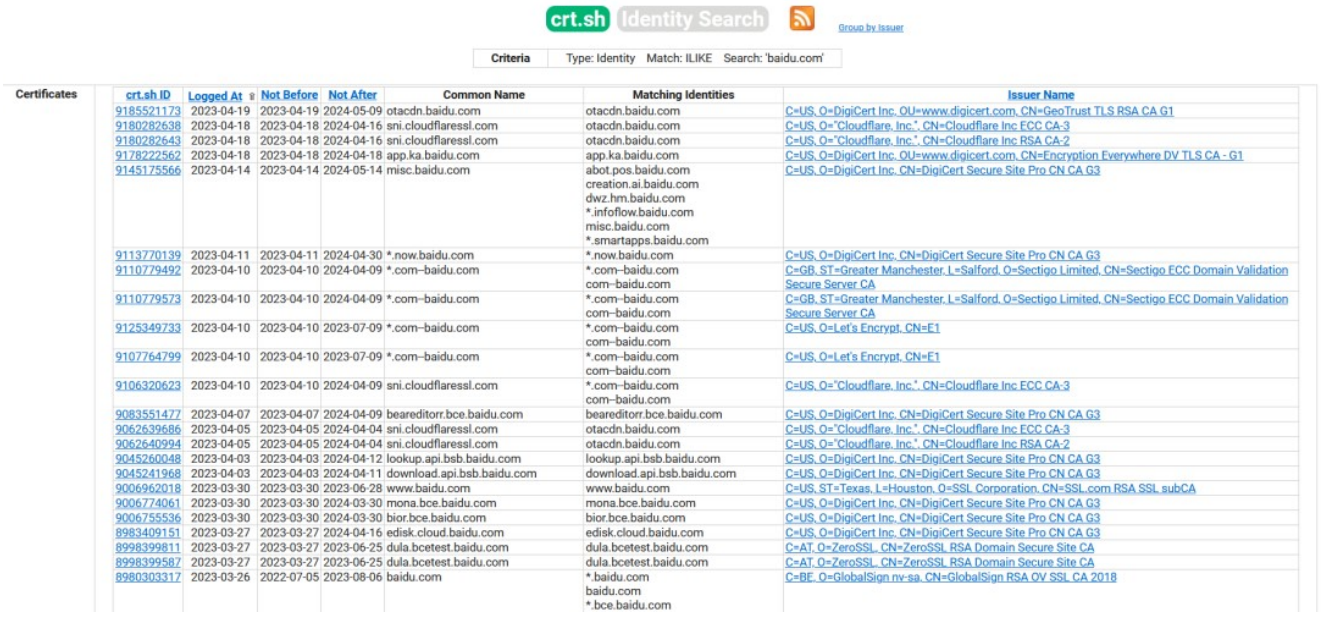
证书透明度 是一个开放体系，专门记录、审核并监控在互联网公开受信任的 TLS 证书。通过这个工具，你可以搜索为特定域名签发的证书，并订阅有关新证书签发和潜在钓鱼攻击的 Facebook 通知。

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	显示详情 (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	显示详情 (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	显示详情 (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	显示详情 (CT Precertificate)
creation.ai.baidu.com infoflow.baidu.com bceidaas.com				

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



crt.sh Identity Search Group by Issuer

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 *.infoflow.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
9006774061	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	bior.bce.baidu.com	bior.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.bcetest.baidu.com	dula.bcetest.baidu.com	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
8998399587	2023-03-27	2023-03-27	2023-06-25	dula.bcetest.baidu.com	dula.bcetest.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