@rcelpe

## 子域枚举的意义

这不是一个新鲜的技术，它的存在是为了增加发现漏洞的概率，
服务于一次渗透测试的成功。

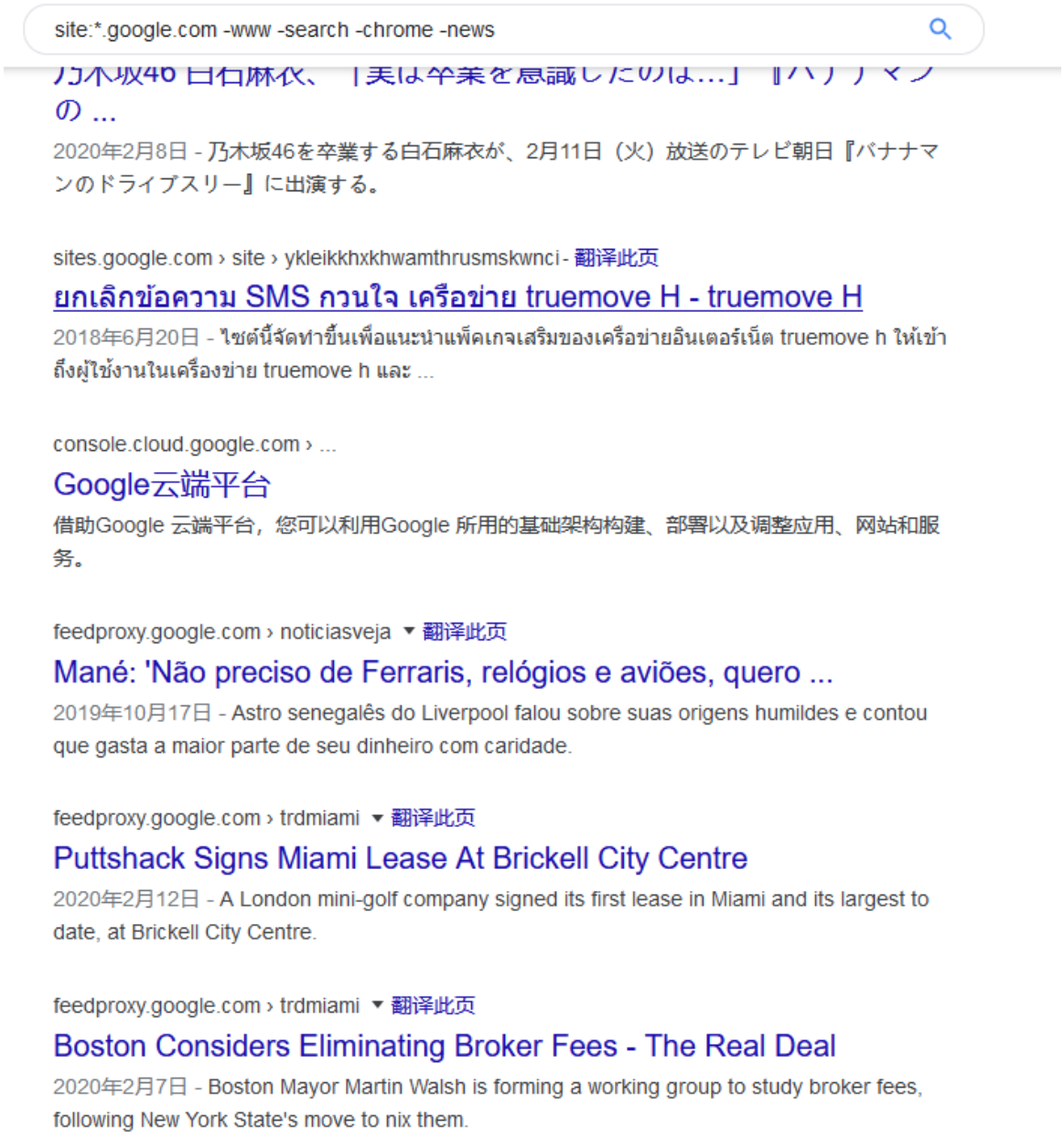
- 子域往往运行着许多应用程序，增加漏洞发现的机会
- 相同的漏洞往往会出现在不同的子域之中
- 隐藏的子域经常会存在重要的应用程序，如果发现关键漏洞可以直击目标核心

## 子域枚举技术详解

### 1.通过搜索引擎

Google语法例如" site:* " 是一种众所周知的方法，它可以用在所有搜索引擎上，
但在Google上支持运算符可以帮助我们排除不感兴趣的子域,

```
site:*.google.com -www -search -chrome -news
```




## 2.通过第三方服务的DNS数据集检索给定域的子域

```
VirusTotal:https://www.virustotal.com/gui/home/search
DNSdumpster:https://dnsdumpster.com/
```

virustotal最初由Hispasec维护是一个免费对可疑文件和网址进行快速检索的在线应用，它检索出的信息比搜索引擎查找的更加直观和全面，不仅可以找到子域还可以找例如whois之类的其它对于网站重要的信息，对于信息侦察阶段具有参考意义。

**Passive DNS Replication**

| Date resolved | IP |
|---|---|
| 2020-02-19 | 172.217.22.142 |
| 2020-02-19 | 216.58.215.46 |
| 2020-02-19 | 172.217.18.206 |
| 2020-02-19 | 216.58.198.206 |
| 2020-02-19 | 216.58.204.110 |
| 2020-02-19 | 172.217.19.238 |
| 2020-02-15 | 216.58.206.238 |
| 2020-02-15 | 216.58.204.142 |
| 2020-02-13 | 216.58.201.238 |
| 2020-02-13 | 172.217.172.142 |

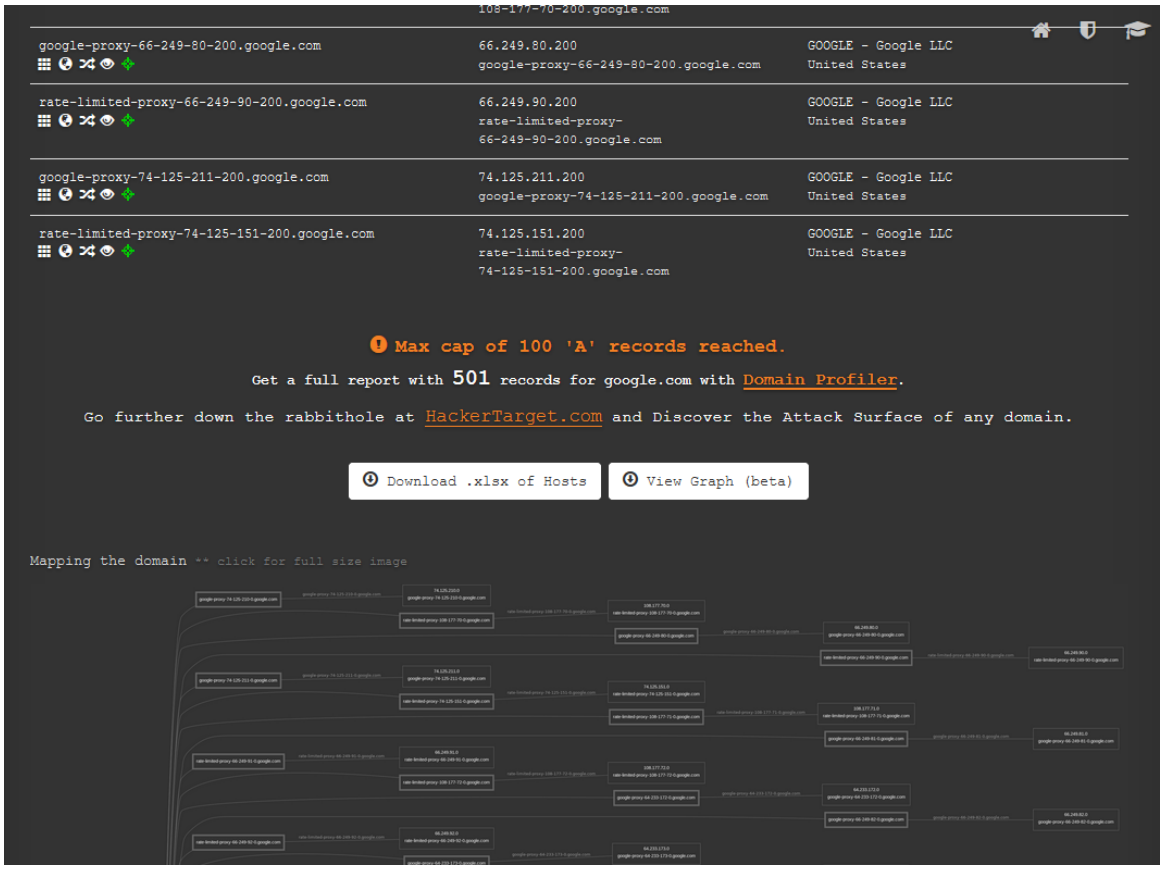
• • •

**Subdomains**

| | | | | |
|---|---|---|---|---|
| get.google.com | 172.217.219.101 | 172.217.219.139 | 172.217.219.102 | ... |
| www.google.com | 216.58.209.228 | 172.217.18.196 | 216.58.213.132 | ... |
| services.google.com | 209.85.146.113 | 172.217.18.238 | 172.217.212.100 | ... |
| consent.google.com | 192.55.83.30 | 192.41.162.30 | 192.52.178.30 | ... |
| fundingchoicesmessages.google.com | 173.194.194.138 | 216.58.198.46 | 172.217.23.14 | ... |
| youtube-ui.l.google.com | 108.177.96.91 | 172.253.120.198 | 172.253.123.190 | ... |
| ads.google.com | 142.250.9.101 | 142.250.9.102 | 142.250.9.100 | ... |
| lh3.google.com | 216.58.207.174 | 216.58.198.78 | 172.217.214.139 | ... |
| mt.google.com | 172.217.219.100 | 172.217.219.102 | 172.217.219.138 | ... |
| sb-ssl.google.com | 216.58.213.142 | 172.217.23.110 | 216.58.207.238 | ... |

DNSdumpster的好处是有一个Mapping，

https://dnsdumpster.com/static/map/google.com.png

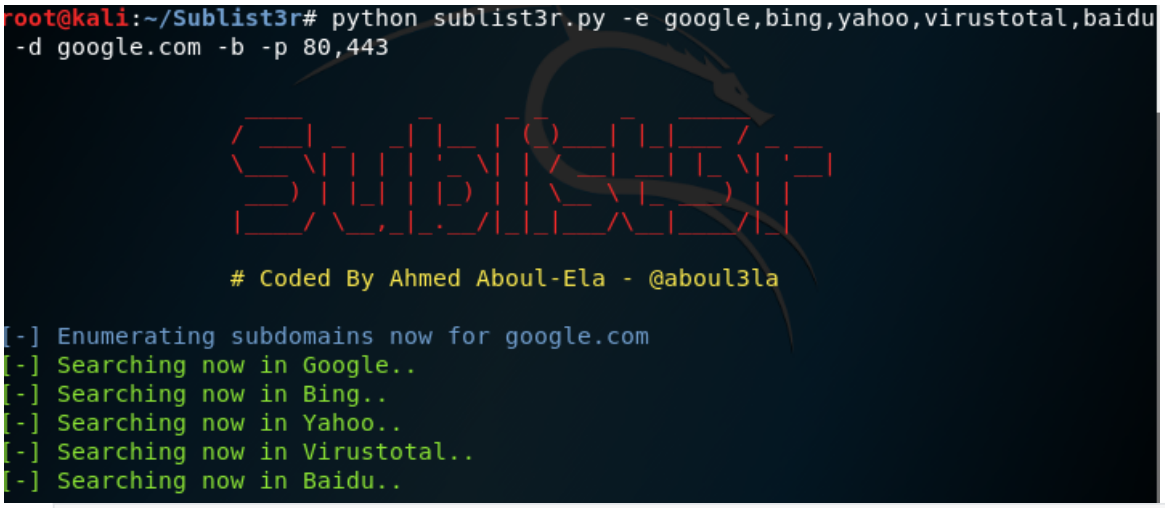



## 3.工具枚举

```
Sublist3r: https://github.com/aboul3la/Sublist3r
```

Sublist3r是一款优秀的工具，它不仅可以枚举子域，还添加了搜索引擎如"Google"、“Yahoo”、“Bing”、“Ask”、甚至是“Baidu”，如果你熟悉网络防火墙在这里可以意识到你需要挂载一个
流量代理，或者使用海外的远程服务器才能发挥它所有的功能，同时它还使用了Netcraft,Virustotal,ThreatCrowd,DNSdumpster,ReverseDNS来枚举子域，所以这是一个“all in one”的工具。

```
python sublist3r.py -e google,bing,yahoo,virustotal -d example.com -b -p 80,443
```



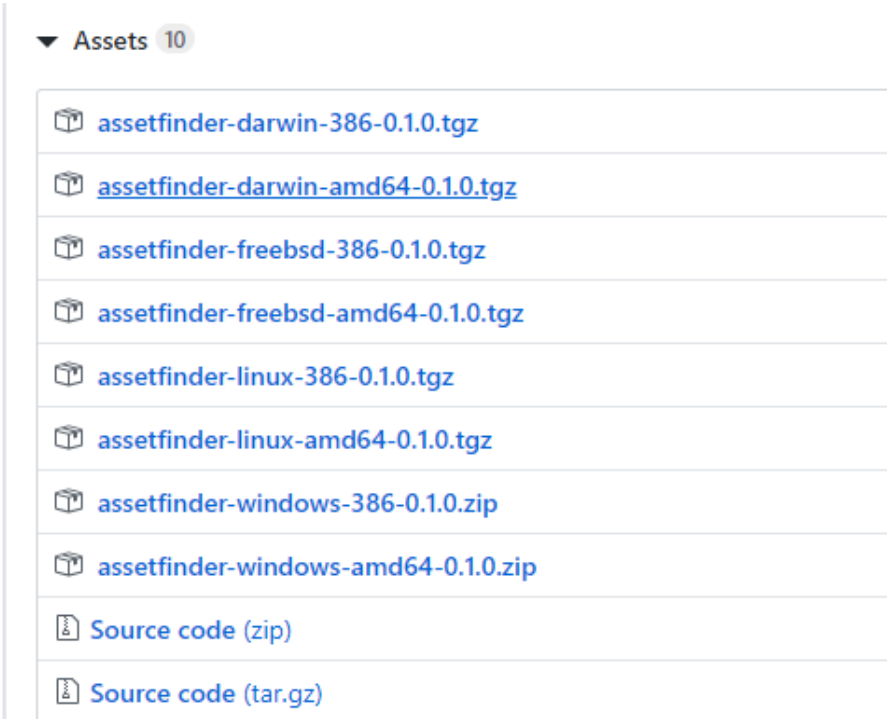

```
-e:是指定搜索引擎
-b:是Brute俗称爆破
-p:是指定端口
```

## Usage

| Short Form | Long Form | Description |
|---|---|---|
| -d | --domain | Domain name to enumerate subdomains of |
| -b | --bruteforce | Enable the subbrute bruteforce module |
| -p | --ports | Scan the found subdomains against specific tcp ports |
| -v | --verbose | Enable the verbose mode and display results in realtime |
| -t | --threads | Number of threads to use for subbrute bruteforce |
| -e | --engines | Specify a comma-separated list of search engines |
| -o | --output | Save the results to text file |
| -h | --help | show the help message and exit |

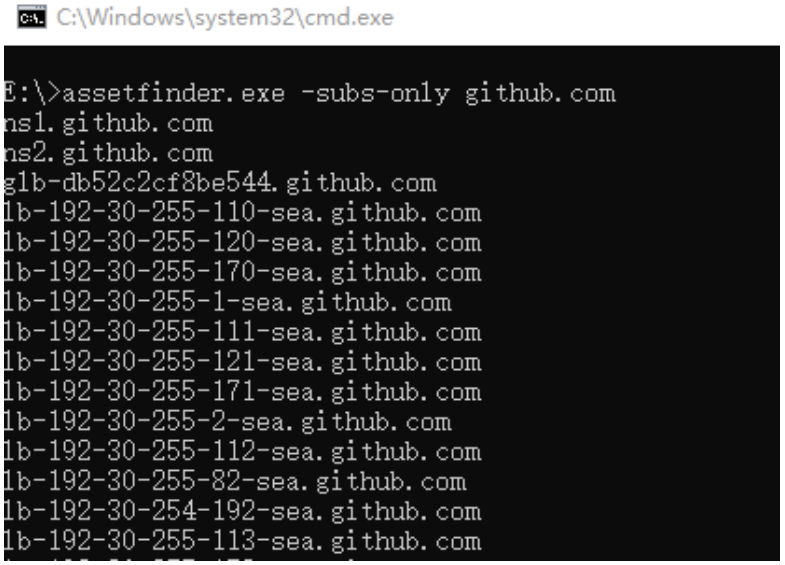
我建议阅读项目的说明文档，这样便于真正的灵活使用它。

```
assetfinder (https://github.com/tomnomnom/assetfinder)
https://github.com/tomnomnom/assetfinder/releases
assetfinder [--subs-only] <domain>
```



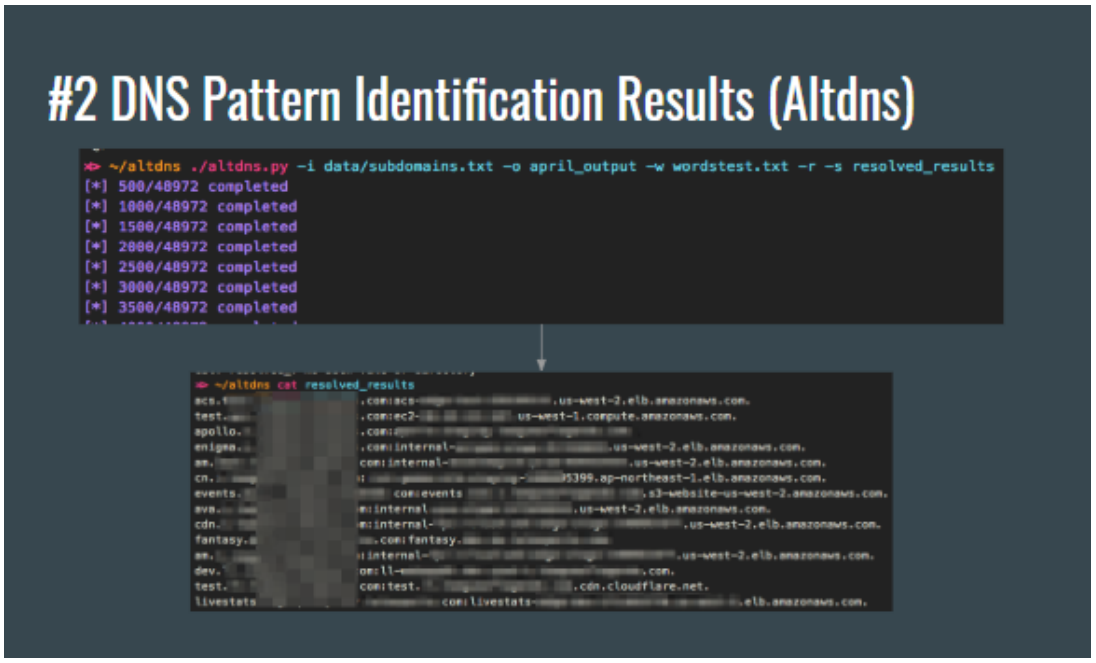

这款子域枚举工具的平台支持性十分良好，而且速度十分优异，

我下载了二进制文件直接可以在Windows下使用，




```
1 altdns: https://github.com/infosec-au/altdns
```

Altdns是一个DNS侦查工具,通过变更和排列允许发现符合模式的子域的工具




类似的工具还有dnsrecon:https://github.com/darkoperator/dnsrecon作为一个dns枚举脚本

## 4.Certificate Transparency(CT)

证书透明度（CT）旨在记录、审核和监视证书颁发机构（CA）(https://en.wikipedia.org/wiki/Certificate_authority)颁发的证书，
CT允许网站用户和域所有者识别错误的或者被恶意修改的颁发证书，
这有助于识别未授权的CA，CA是受信任的第三方，受数字证书的所有者和依赖证书的一方的信任，
证书颁发机构CA会颁发每个SSL/TLS证书发布到公共日志中，
SSL/TLS证书通常会包含域名、子域、电子邮件这些对攻击者有价值的信息，
如果你要成为理论专家，我建议你阅读（https://blog.appsecco.com/certificate-transparency-the-bright-side-and-the-dark-side-8aa47d9a6616）

### (1)crt.sh

```
https://crt.sh/?q=%25.example.com
```

crt.sh Identity Search Group by Issuer

Criteria | Type: Identity Match: ILIKE Search: 'google.com'

Certificates

| crt.sh ID | Logged At | Not Before | Not After | Matching Identities | Issuer Name |
|---|---|---|---|---|---|
| 2381394777 | 2020-01-27 | 2011-07-13 | 2012-07-13 | *.docs.google.com<br>*.mail.google.com<br>*.plus.google.com<br>*.sites.google.com<br>*.talkgadget.google.com | C=US, O=Google Inc, CN=Google Internet Authority |
| 2380986199 | 2020-01-26 | 2011-02-16 | 2012-02-16 | *.docs.google.com<br>*.mail.google.com<br>*.sites.google.com<br>*.talkgadget.google.com | C=US, O=Google Inc, CN=Google Internet Authority |
| 2380850988 | 2020-01-26 | 2012-02-29 | 2013-02-28 | onex.wifi.google.com | C=US, O=Google Inc, CN=Google Internet Authority |
| 2380841885 | 2020-01-26 | 2011-07-13 | 2012-07-13 | accounts.google.com | C=US, O=Google Inc, CN=Google Internet Authority |
| 2380681291 | 2020-01-26 | 2013-11-22 | 2013-11-24 | hosted-id.google.com | C=US, O=Google Inc, CN=Google Internet Authority G2 |
| 2380579544 | 2020-01-26 | 2011-05-11 | 2012-05-11 | accounts.google.com | C=US, O=Google Inc, CN=Google Internet Authority |
| 2379825238 | 2020-01-26 | 2011-05-11 | 2012-05-11 | adwords.google.com<br>adwords.google.com.ar | C=US, O=Google Inc, CN=Google Internet Authority |

crt.sh提供PostgreSQL接口来提权给定域名的子域

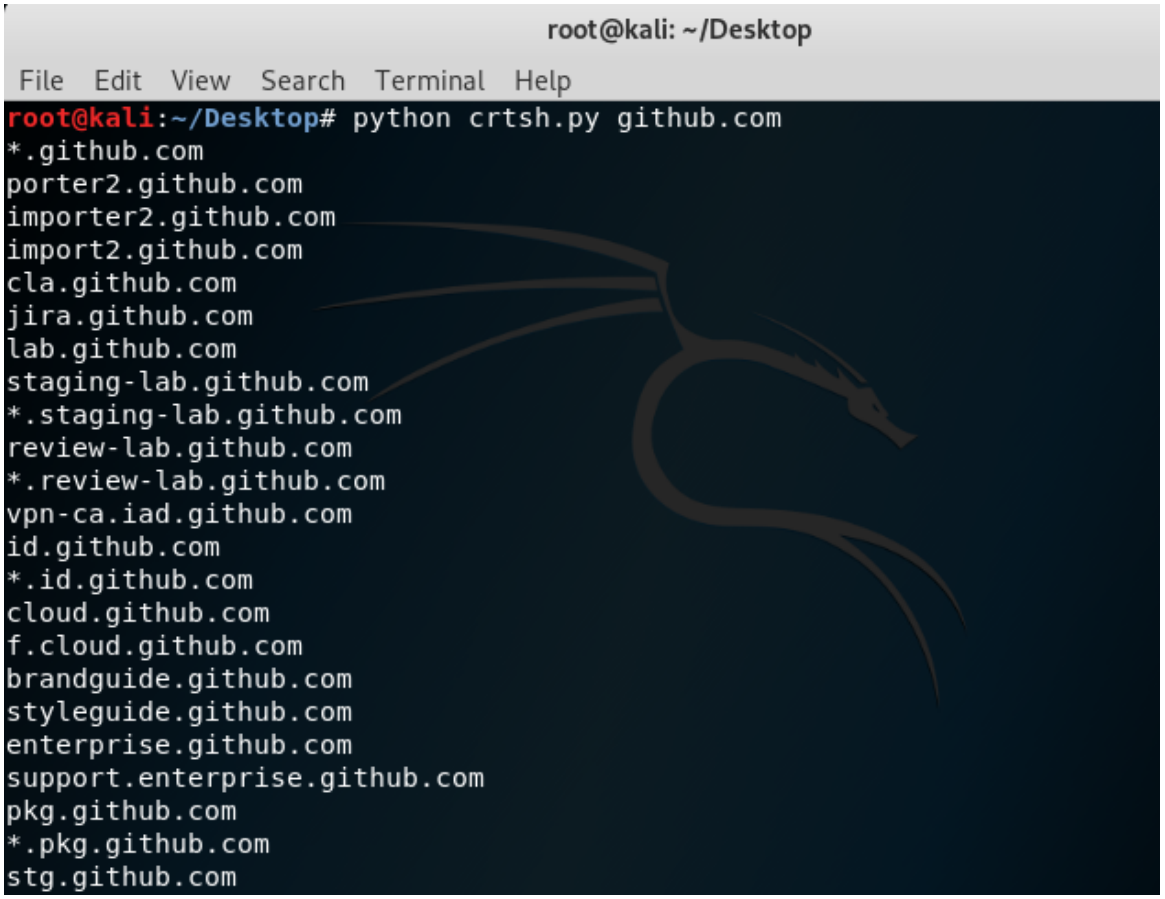
```
#!/bin/sh

# Script by Hanno Bock - https://github.com/hannob/tlshelpers/blob/master/getsubdomain

query="SELECT ci.NAME_VALUE NAME_VALUE FROM certificate_identity ci WHERE ci.NAME_TYPE = 'dNSName' AND reverse(lower(ci.NAME_VALUE)) LIKE reverse(lower('%.$1'));"

echo $query | \
 psql -t -h crt.sh -p 5432 -U guest certwatch | \
 sed -e 's:^ *::g' -e 's:^*\.::g' -e '/^$/d' | \
  sort -u | sed -e 's:*.::g'
```

也可以使用python脚本



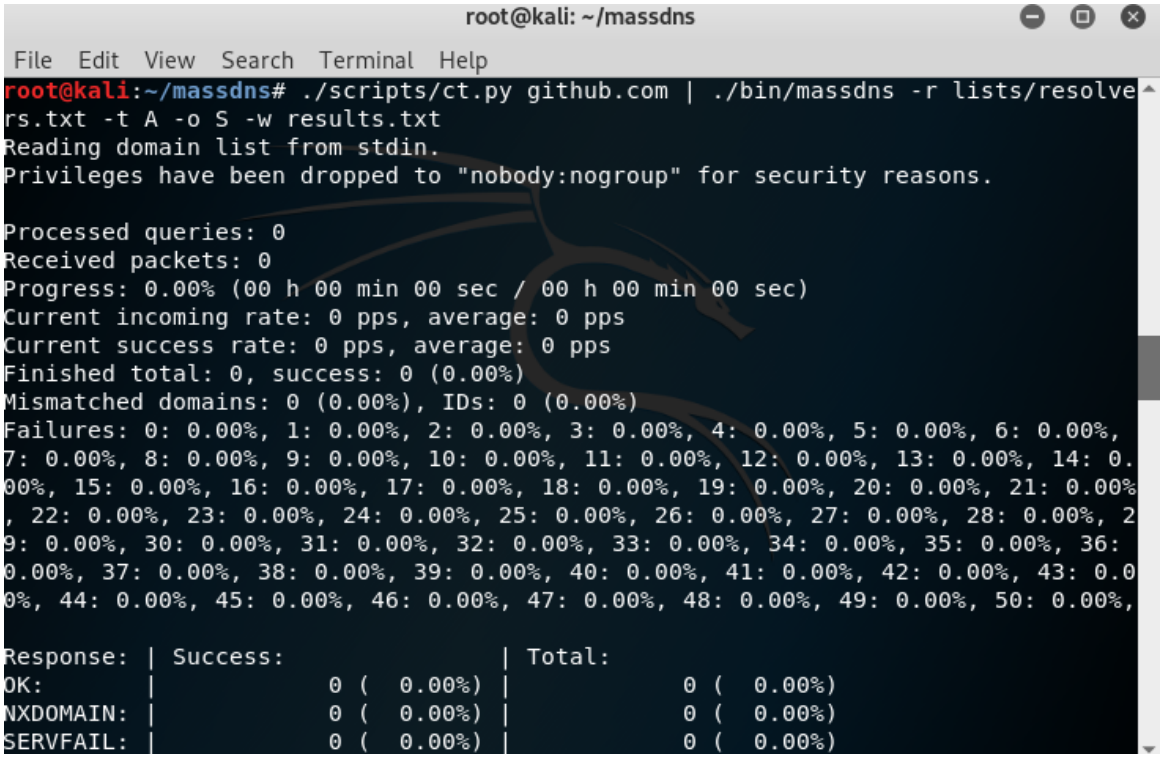

优秀的研究人员把更多的ct搜索脚本放在这里
(https://github.com/appsecco/the-art-of-subdomain-enumeration)

**(2)massdns(https://github.com/blechschmidt/massdns)**

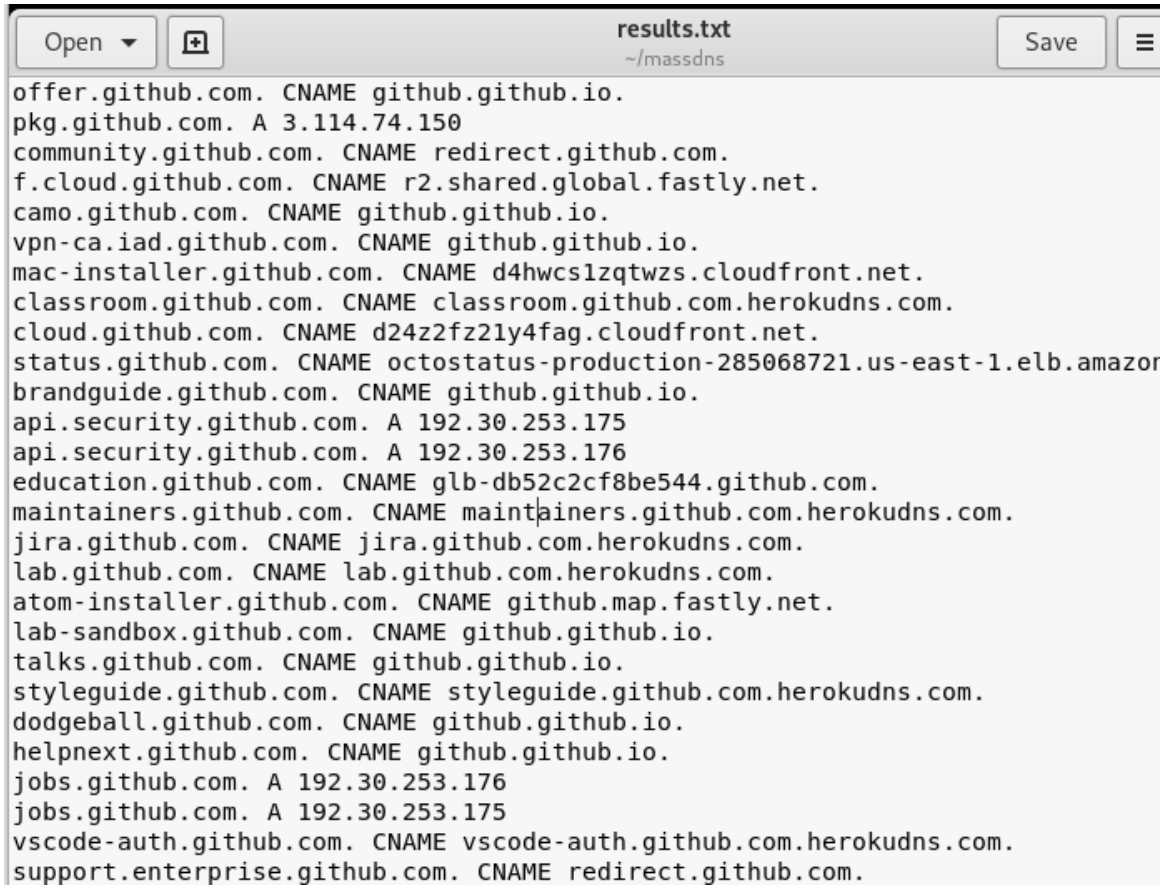
该项目使用前需要进行编译，在根目录下运行make即可

massdns支持crt.sh使用

```
./scripts/ct.py github.com | ./bin/massdns -r lists/resolvers.txt -t A -o S -w r
esults.txt
```

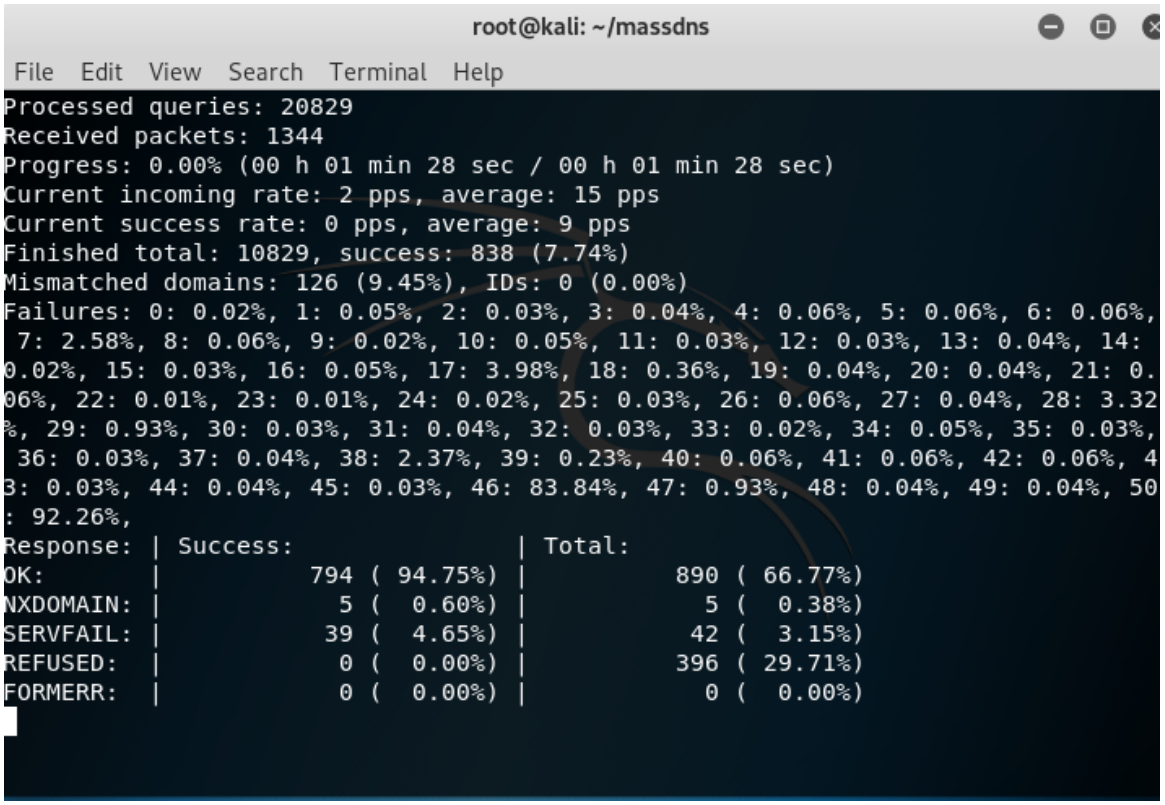



保存结果的文件在目录下




script目录下的(subbrute.py)支持对子域进行暴力枚举

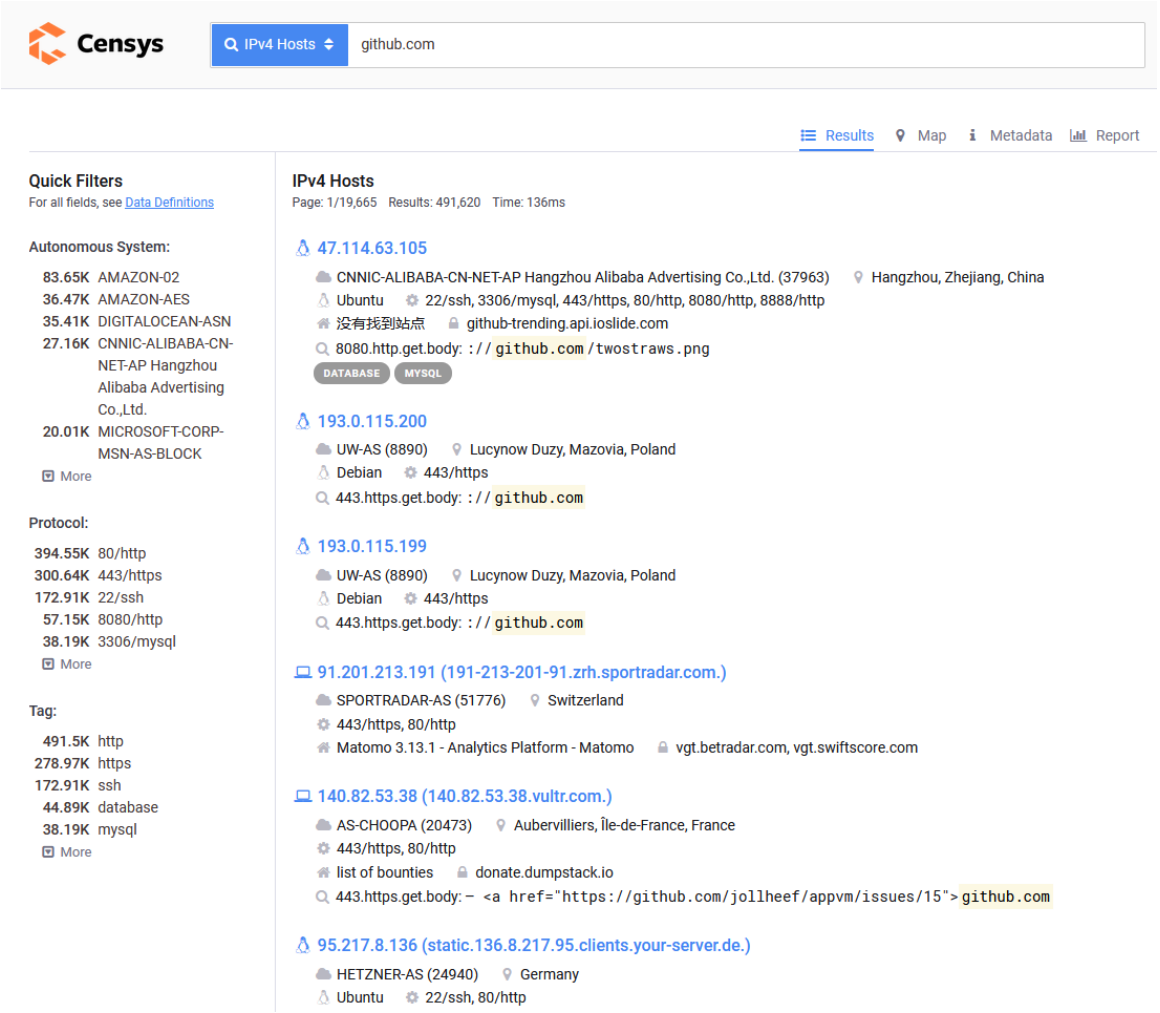
```
./scripts/subbrute.py lists/names.txt github.com | ./bin/massdns -r lists/resolv
ers.txt -t A -o S -w results.txt
```




**(3)censys**

censys是跟shodan同种类的搜索引擎，黑客可以用来做信息侦察，安全人员可以拿来做安全研究

```
https://censys.io/ipv4?q=example.com
```



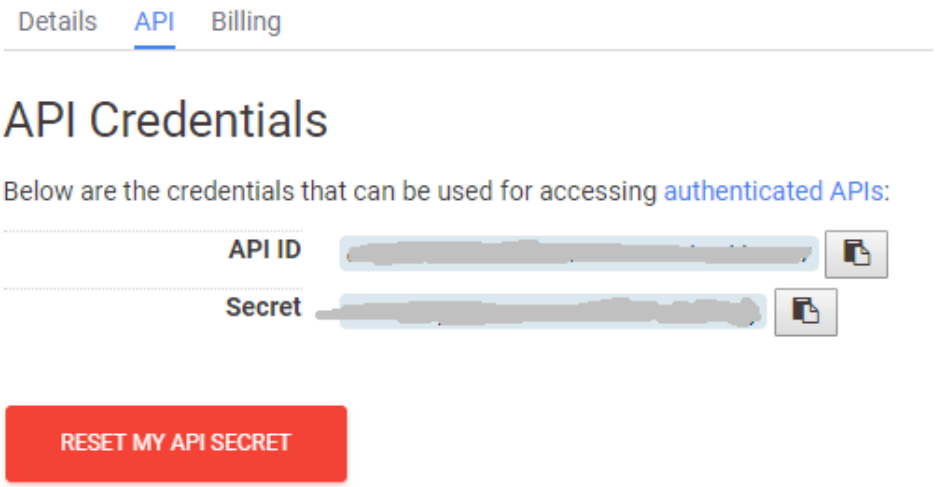

同时也可以用censys python库编写的工具来提取给定域的子域

```
https://github.com/christophetd/censys-subdomain-finder
https://github.com/0xbharath/censys-enumeration
```

使用这类工具通常都需要设置API，

这里需要先注册一个账户在https://censys.io/register

注册是免费的，然后访问https://censys.io/account/api



并且使用你注册账户的API ID和API Secret设置两个环境变量

```
$ export CENSYS_API_ID="********"
$ export CENSYS_API_SECRET="********"
```

值得一提的是censys_enumeration可以枚举子域和邮箱，用法如下：

```
$ python censys_enumeration.py domains.txt
```

censys_subdomain_finder:

```
$ python censys_subdomain_finder.py example.com
[*] Searching Censys for subdomains of example.com
[*] Found 5 unique subdomains of example.com

- products.example.com
- www.example.com
- dev.example.com
- example.com
- support.example.com
```

5.自治系统/自治域(Autonomous system, AS)

> 自治系统是指在互联网中，一个或多个实体管辖下的所有IP网络和路由器的组合，它们对互联网执行共同的路由策略,参看RFC 1930中更新的定义。

```
https://tools.ietf.org/html/rfc1930
https://en.wikipedia.org/wiki/Autonomous_system_(Internet)
https://www.iana.org/assignments/as-numbers/as-numbers.xhtml
```

通过查找自治系统(AS)编号可以帮助我们识别某个组织的网络块具有的有效域，

```
https://asn.cymru.com/cgi-bin/whois.cgi
https://www.ultratools.com/tools/asnInfo
https://nmap.org/nsedoc/scripts/targets-asn.html
```

Family: ◉ IPv4 ○ IPv6 Methods: ☑ whois ☑ peer-whois
Flags: ☑ prefix ☑ cc ☑ registry ☑ allocated ☑ notruncate ☑ verbose

13.229.188.59

Insert your IP or ASN in the textbox above.

**IPv4 [OPTIONAL COMMENT]**
Eg. '4.2.2.2 2004-12-10 11:33:21 GMT'

**AS#**
Eg. 'AS23028'

**IPv6 [OPTIONAL COMMENT]**

--- snip snip ---
2001:5c0:8fff:fffe::ff6 2004-12-10 11:32:01 GMT
2001:5c0:8fff:fffe::ff7 2004-12-10 11:33:21 GMT
--- snip snip ---

Both IPv4 and IPv6 addresses are supported.
However, only one address family is permitted
per query. In other words, you may NOT intermix
IPv4 and IPv6 addresses.

Submit Reset

---

**Executing commands. Please be patient!**

**v4.whois.cymru.com**

The server returned 2 line(s).

```
AS      | IP               | BGP Prefix          | CC | Registry | Allocated  | AS Name
16509   | 13.229.188.59    | 13.228.0.0/15       | US | arin     | 2016-08-09 | AMAZON-02, US
```

**v4-peer.whois.cymru.com**

The server returned 3 line(s).

```
PEER_AS | IP               | BGP Prefix          | CC | Registry | Allocated  | AS Name
2914    | 13.229.188.59    | 13.228.0.0/15       | US | arin     | 2016-08-09 | NTT-COMMUNICATIONS-2914, US
6453    | 13.229.188.59    | 13.228.0.0/15       | US | arin     | 2016-08-09 | AS6453, US
```

---

Email Share

# ASN Lookup & Information

The ASN Information tool provides complete autonomous system (AS) information.

Autonomous Systems are routable networks within the public Internet, administered by the local RIRs and assigned to owners of networks. The ASN Information tool displays information about an IP address's Autonomous System Number (ASN) such as: IP owner, registration date, issuing registrar and the max range of the AS with total IPs.

*Enter an AS number, IP address, or a Company name.*

16509 Go »

*Related Tools:* CIDR/Netmask What's your IP Decimal IP Calculator

AS16509

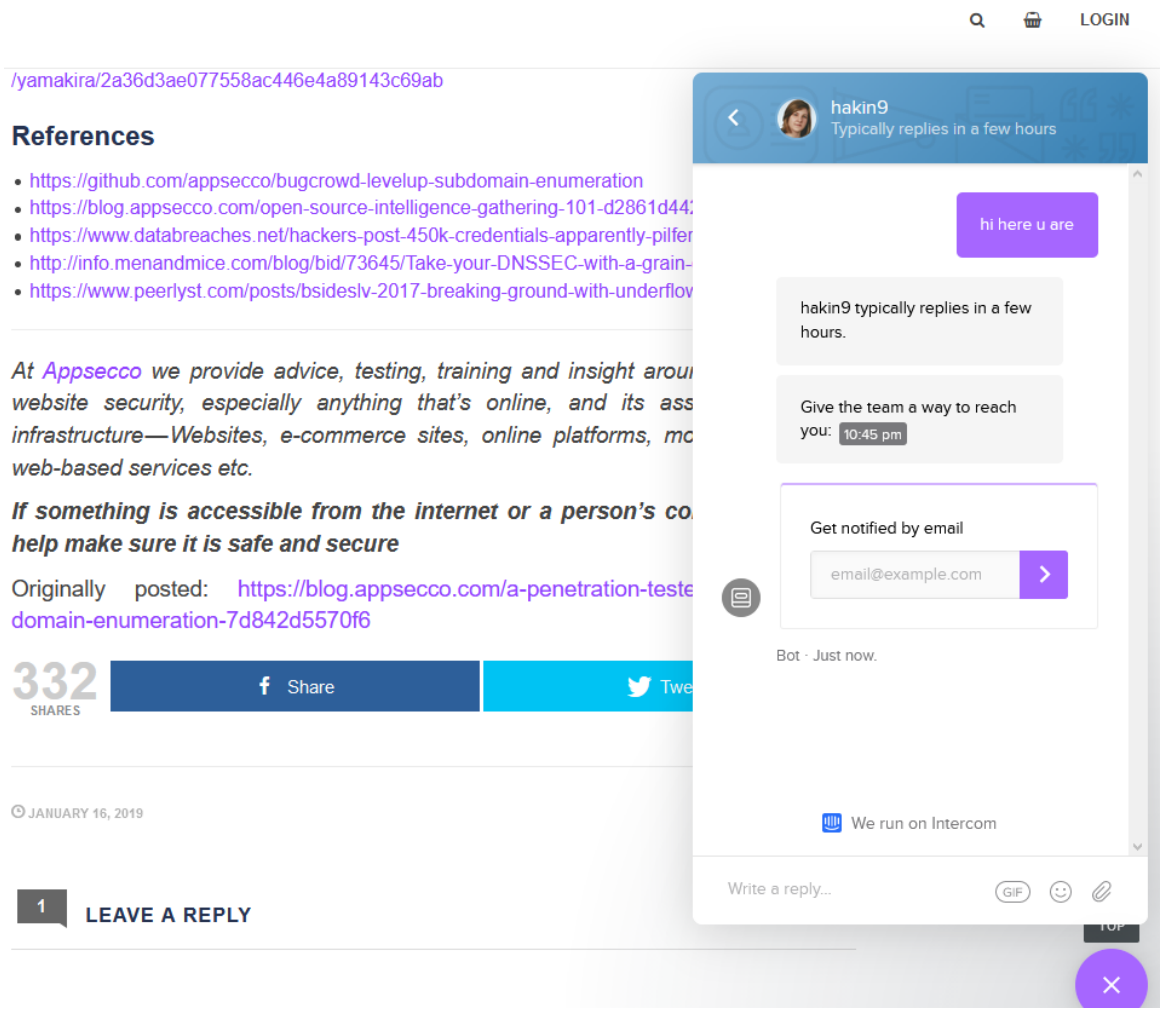
```
           Country: US
  Registration Date: 2000-05-04
         Registrar: arin
             Owner: AMAZON-02, US
```

找到的ASN编号可以使用nmap脚本来查找域的网块

```
1 nmap --script targets-asn --script-args targets-asn.asn=ASN编号
```

```
C:\Users\Administrator>nmap --script targets-asn --script-args targets-asn.asn=16509
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-23 23:35 ?D1ú±ê×?ê±??
Pre-scan script results:
| targets-asn:
|   16509
|     3.0.0.0/15
|     3.5.128.0/24
|     3.5.129.0/24
|     3.5.130.0/24
|     3.5.128.0/22
|     3.5.131.0/24
|     3.5.132.0/24
|     3.5.132.0/23
|     3.5.133.0/24
|     3.5.208.0/24
|     3.5.209.0/24
|     3.5.210.0/24
|     3.5.208.0/22
|     3.5.211.0/24
|     3.5.212.0/24
|     3.5.212.0/23
|     3.5.213.0/24
|     3.6.0.0/15
|     3.8.0.0/14
|     3.12.0.0/16
```

还有其它“花哨”的手段可以阅读参考书(https://hakin9.org/a-penetration-testers-guide-to-subdomain-enumeration/)进行学习补充，hakin9提供了在线答疑功能，当你有疑虑的时候可以直击右下角进行询问在线答疑人员。




## 实例参考:

> 本例子引用了h1中的一个报告(https://hackerone.com/reports/770513)

## (1)首先通过crt.sh来查找存在多级子域的目标

crt.sh Identity Search Group by Issuer

Criteria | Type: Identity Match: ILIKE Search: '%.%.%.%.8x8.com'

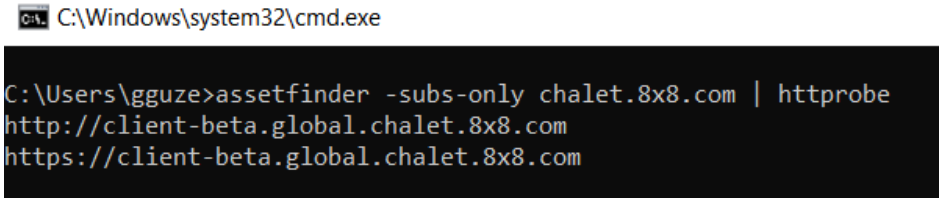
ertificates

| crt.sh ID | Logged At | Not Before | Not After | Matching Identities | Issuer Name |
|---|---|---|---|---|---|
| 1862945263 | 2019-09-09 | 2019-08-28 | 2020-09-28 | *.prod.us-east-1.ai.8x8.com | C=US, O=Amazon, OU=Server CA 1B, CN=Amazon |
| 1822044596 | 2019-08-29 | 2019-08-22 | 2020-09-22 | *.dev.us-east-1.ai.8x8.com | C=US, O=Amazon, OU=Server CA 1B, CN=Amazon |
| 1817385556 | 2019-08-28 | 2019-08-28 | 2020-09-28 | *.prod.us-east-1.ai.8x8.com | C=US, O=Amazon, OU=Server CA 1B, CN=Amazon |
| 1795729913 | 2019-08-22 | 2019-08-22 | 2020-09-22 | *.dev.us-east-1.ai.8x8.com | C=US, O=Amazon, OU=Server CA 1B, CN=Amazon |
| 1812431063 | 2019-08-08 | 2019-08-08 | 2019-11-06 | *.100.us-east-1.acceptance.cloud.8x8.com | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 1751791851 | 2019-08-08 | 2019-08-08 | 2019-11-06 | *.100.us-east-1.acceptance.cloud.8x8.com | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 1812427214 | 2019-08-08 | 2019-08-08 | 2019-11-06 | *.01.us-east-1.acceptance.cloud.8x8.com | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 1751788043 | 2019-08-08 | 2019-08-08 | 2019-11-06 | *.01.us-east-1.acceptance.cloud.8x8.com | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 1812306711 | 2019-08-08 | 2019-08-08 | 2019-11-06 | *.01.us-east-1.acceptance.cloud.8x8.com | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 1751701394 | 2019-08-08 | 2019-08-08 | 2019-11-06 | *.01.us-east-1.acceptance.cloud.8x8.com | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 1443087767 | 2019-05-07 | 2019-05-07 | 2020-06-07 | *.qa.us-east-1.ai.8x8.com *.stg.us-east-1.ai.8x8.com | C=US, O=Amazon, OU=Server CA 1B, CN=Amazon |
| 804503927 | 2018-10-01 | 2018-09-26 | 2019-10-26 | *.prod.us-east-1.ai.8x8.com | C=US, O=Amazon, OU=Server CA 1B, CN=Amazon |
| 803946172 | 2018-10-01 | 2018-09-20 | 2019-10-20 | *.dev.us-east-1.ai.8x8.com | C=US, O=Amazon, OU=Server CA 1B, CN=Amazon |
| 788922624 | 2018-09-26 | 2018-09-26 | 2019-10-26 | *.prod.us-east-1.ai.8x8.com | C=US, O=Amazon, OU=Server CA 1B, CN=Amazon |
| 770132733 | 2018-09-20 | 2018-09-20 | 2019-10-20 | *.dev.us-east-1.ai.8x8.com | C=US, O=Amazon, OU=Server CA 1B, CN=Amazon |
| 315064848 | 2018-01-28 | 2018-01-28 | 2018-04-28 | sip1.sw.us-east.chalet.8x8.com | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 266645760 | 2017-11-29 | 2017-11-29 | 2018-02-27 | sip1.sw.us-east.chalet.8x8.com | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 220666504 | 2017-09-30 | 2017-09-30 | 2017-12-29 | sip1.sw.us-east.chalet.8x8.com | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |


| 315064848 | 2018-01-28 | 2018-01-28 | 2018-04-28 | sip1.sw.us-east.chalet.8x8.com |
|---|---|---|---|---|
| 266645760 | 2017-11-29 | 2017-11-29 | 2018-02-27 | sip1.sw.us-east.chalet.8x8.com |
| 220666504 | 2017-09-30 | 2017-09-30 | 2017-12-29 | sip1.sw.us-east.chalet.8x8.com |


## (2)接着使用assetfinder配合httprobe来枚举子域

```
https://github.com/tomnomnom/assetfinder/releases
https://github.com/tomnomnom/httprobe/releases
```




将目标锁定为https://client-beta.global.chalet.8x8.com/

## (3)用dirsearch来进行目录探测

```
https://github.com/maurosoria/dirsearch
```

```
F:\dirsearch>python dirsearch.py -b -u "https://client-beta.global.chalet.8x8.com/" -e html,json

 _|. _ _  _  _  _ _|_    v0.3.9
(_||| _) (/_(_|| (_| )

Extensions: html, json | HTTP method: get | Threads: 10 | Wordlist size: 6422

Error Log: F:\dirsearch\logs\errors-20-02-23_23-07-30.log

Target: https://client-beta.global.chalet.8x8.com/

[23:07:31] Starting:
[23:07:44] 400 -  915B  - /%2e%2e/google.com
[23:07:47] 400 -  277B  - /%ff/
[23:12:08] 200 -   15KB - /favicon.ico
[23:12:57] 200 -    5KB - /index.html
[23:13:47] 200 -  412B  - /manifest.json
[23:14:16] 200 -   97B  - /oauth
[23:17:06] 200 -    0B  - /soap/

Task Completed
```


:bad_params

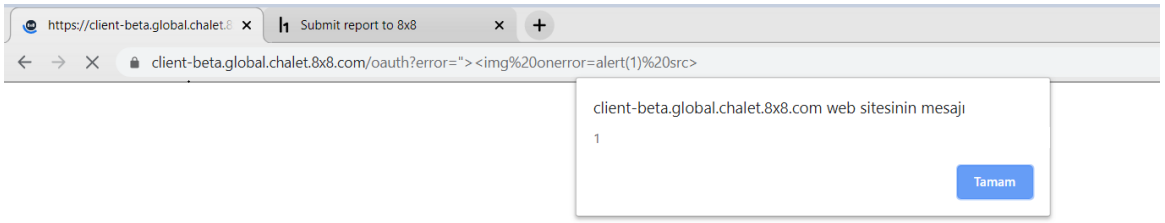
Back

### (4)使用arjun查找隐藏参数

```
1 https://github.com/s0md3v/Arjun
```


### (5)插入Payload获得xss

```
1 Payload : "><img onerror=alert(1) src>
```




## 参考来源:

> https://censys.io/

https://crt.sh/
https://www.virustotal.com/gui/home/search
https://dnsdumpster.com/
https://github.com/aboul3la/Sublist3r
https://github.com/tomnomnom/assetfinder/releases
https://github.com/infosec-au/altdns
https://github.com/darkoperator/dnsrecon
https://en.wikipedia.org/wiki/Certificate_authority
https://blog.appsecco.com/certificate-transparency-the-bright-side-and-the-dark-side-8aa47d9a6616
https://docs.google.com/presentation/d/1PCnjzCeklOeGMoWiE2IUzlRGOBxNp8K5hLQuvBNzrFY/edit
https://github.com/appsecco/bugcrowd-levelup-subdomain-enumeration
https://blog.appsecco.com/open-source-intelligence-gathering-101-d2861d4429e3
https://www.databreaches.net/hackers-post-450k-credentials-apparently-pilfered-from-yahoo/
http://info.menandmice.com/blog/bid/73645/Take-your-DNSSEC-with-a-grain-of-salt
https://hakin9.org/a-penetration-testers-guide-to-subdomain-enumeration/
https://medium.com/@gguzelkokar.mdbf15/get-reflected-xss-within-3-minutes-baa314e25489
https://www.peerlyst.com/posts/bsideslv-2017-breaking-ground-with-underflow-bsides-las-vegas
https://github.com/appsecco/the-art-of-subdomain-enumeration
https://github.com/blechschmidt/massdns
https://github.com/christophetd/censys-subdomain-finder
https://github.com/0xbharath/censys-enumeration
https://tools.ietf.org/html/rfc1930
https://en.wikipedia.org/wiki/Autonomous_system_(Internet)
https://www.iana.org/assignments/as-numbers/as-numbers.xhtml
https://asn.cymru.com/cgi-bin/whois.cgi
https://www.ultratools.com/tools/asnInfo
https://nmap.org/nsedoc/scripts/targets-asn.html