子域名挖掘工具

一、子域名为什么重要

子域名是许多攻击技术的有效媒介和踏板，无论是针对域名进行攻击渗透还是对攻击行为进行测绘都离不开这一重要的工具。此外，为了更好的监测网站资源、构建更加完整的域名依赖体系，也需要将子域名考虑在内。获得子域名的方法有许多，例如查寻第三方记录、暴力枚举、基于搜索引擎搜索等。

二、Sublist3r

1. 简介与原理

Sublist3r 是一个基于 python 便携的子域名挖掘工具，基本原理也是利用公开的资源进行查询，主要的搜索手段如下：

1）利用自建的子域名库在线枚举匹配（129408 个流行域名前缀）

2）利用 chrome、yoo、bing、baidu 等浏览器进行查找，查找的思路是利用浏览器信息探测规则（可参考 google 语法）搜索域名，进而通过正则表达式提取页面中的子域，直到提取结束。

具体而言，就是将 site:example.com 这一字符串输入搜索引擎，搜索引擎会返回诸如 a.example.com，b.example.com 等结果，接着利用正则表达式将这些域名提取出来，修改探测规则为：site:example.com -site:a.example.com -site:b.example.com，这一规则的含义是搜索 example.com 的子域，但不包括 a.example.com 和 b.example.com，然后再将修改后的规则字符串输入搜索引擎进行检索，以此类推，直到不再出现新的子域名，这也就是说最后所有的子域名都会包括在探测规则字符串中。

3）利用证书搜索

出于成本的考虑，许多网站的证书保护机制，都是利用一个证书保护所有子域。鉴于这一现象，利用 https://crt.sh 网站可以检索同一证书下的子域，使用方法如下：https://crt.sh/?q=example.com

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
3430918329	2020-09-26	2020-07-23	2021-07-23	sni.cloudflaressl.com	cloudflare-s1-cndtest.bilibili.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
3363873776	2020-09-10	2020-07-23	2021-07-23	sni.cloudflaressl.com	cloudflare-patch-cndtest.bilibili.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
3351350698	2020-09-07	2020-09-07	2020-12-06	maoer.bilibili.com	maoer.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3351348994	2020-09-07	2020-09-07	2020-12-06	maoer.bilibili.com	maoer.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3291744421	2020-08-26	2020-08-26	2022-08-08	*.game.bilibili.com	*.game.bilibili.com game.bilibili.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign GCC R3 DV TLS CA 2020
3268032183	2020-08-20	2020-08-20	2020-11-18	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3268032189	2020-08-20	2020-08-20	2020-11-18	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3267826256	2020-08-20	2020-08-20	2020-11-18	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3267819783	2020-08-20	2020-08-20	2020-11-18	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3223275472	2020-08-11	2020-08-11	2020-11-09	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3223275788	2020-08-11	2020-08-11	2020-11-09	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3196979913	2020-08-07	2020-08-07	2022-08-08	*.game.bilibili.com	*.game.bilibili.com game.bilibili.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA DV SSL CA 2018
3196691431	2020-08-07	2020-08-07	2022-10-19	*.bilibili.com	*.bilibili.com bilibili.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
3127823204	2020-07-23	2020-07-23	2021-07-23	sni.cloudflaressl.com	cloudflare-patch-cndtest.bilibili.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
3127771724	2020-07-23	2020-07-23	2021-07-23	sni.cloudflaressl.com	cloudflare-s1-cndtest.bilibili.com	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
3087063242	2020-07-14	2020-07-14	2020-10-12	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3087063483	2020-07-14	2020-07-14	2020-10-12	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3086697190	2020-07-14	2020-07-14	2020-10-12	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3086697592	2020-07-14	2020-07-14	2020-10-12	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3086661439	2020-07-14	2020-07-14	2020-10-12	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3086657760	2020-07-14	2020-07-14	2020-10-12	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3083550418	2020-07-13	2020-07-13	2020-10-11	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3083550133	2020-07-13	2020-07-13	2020-10-11	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3082552889	2020-07-13	2020-07-13	2020-10-11	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3082546139	2020-07-13	2020-07-13	2020-10-11	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3064654073	2020-07-09	2020-07-09	2020-10-07	maoer.bilibili.com	maoer.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3064654072	2020-07-09	2020-07-09	2020-10-07	maoer.bilibili.com	maoer.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3059744519	2020-07-08	2020-07-08	2020-10-06	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3059744363	2020-07-08	2020-07-08	2020-10-06	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3059264712	2020-07-08	2020-07-08	2020-10-06	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3059260784	2020-07-08	2020-07-08	2020-10-06	leapfrog-ssl-31.gcs-web.com	ir.bilibili.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

图 1 利用 https://crt.sh 网站检索 bilibili.com 子域

4) DNS 搜集

基于第三方的 DNS 查询记录，检索子域名，例如使用 dnsdumpster.com 网站，[1]推测 dnsdumpster 的底层细节，可能是利用域传输漏洞、DNS 反差、暴力枚举。具体使用如下：https://dns.bufferover.run/dns?q=example.com


```
"93.184.216.34,example.com",
"203.180.136.57,iij01-example.com",
"163.49.89.40,ns1.iij03-example.com",
"34.102.136.180,4-example.com",
"91.195.241.136,a-example.com",
"91.195.241.136,www.a-example.com",
"162.241.244.28,test-ga-example.com",
"162.241.244.28,webdisk.test-ga-example.com",
"162.241.244.28,cpanel.test-ga-example.com",
"162.241.244.28,webmail.test-ga-example.com",
"162.241.244.28,autodiscover.test-ga-example.com",
"test-ga-example.com,www.test-ga-example.com",
"94.130.128.163,ra-example.com",
"94.130.128.163,webdisk.ra-example.com",
"94.130.128.163,cpanel.ra-example.com",
"ra-example.com,mail.ra-example.com",
"94.130.128.163,webmail.ra-example.com",
"94.130.128.163,autodiscover.ra-example.com",
"94.130.128.163,cpcalendars.ra-example.com",
"94.130.128.163,cpcontacts.ra-example.com",
"ra-example.com,www.ra-example.com",
"74.220.199.6,trifecta-example.com",
"74.220.199.6,webdisk.trifecta-example.com",
"74.220.199.6,cpanel.trifecta-example.com",
"74.220.199.6,mail.trifecta-example.com",
"74.220.199.6,webmail.trifecta-example.com",
"74.220.199.6,autodiscover.trifecta-example.com",
"74.220.199.6,www.trifecta-example.com",
"91.195.241.136,b-example.com",
"91.195.241.136,www.b-example.com",
"49.212.198.14,web-example.com",
"49.212.198.14,solution.web-example.com",
"solution.web-example.com,www.solution.web-example.com",
"web-example.com,www.web-example.com",
"217.182.171.203,rb-example.com",
"217.182.171.203,www.rb-example.com",
"204.194.23.4,dnssec-example.com",
"204.194.23.4,www.dnssec-example.com",
```


图 2 利用 dnsdumpster.com 检索 bilibili.com 子域

2.安装与使用

下载地址：git clone https://github.com/aboul3la/Sublist3r.git

使用方式：命令行

命令格式：python sublist3r.py -d example.com

参数解释：-d -domain 要枚举子域的域名

-b -bruteforce 启用 subbrute bruteforce 模块

-p -ports 根据特定的 tcp 端口扫描找到的子域

-v --verbose 启用详细模式并实时显示结果

-t -threads 用于 subbrute bruteforce 的线程数

-e - 引擎指定逗号分隔的搜索引擎列表

-o -output 将结果保存到文本文件

-h -help 显示帮助信息并退出

使用注意：建议 python2，亲测 python3，需将 sublist3r.py 文件第 616 行：

```
ip = Resolver.query(host, 'A')[0].to_text()
```

修改为：`ip = dns.resolver.Resolver.resolve(host, 'A')[0].to_text()`

303 行 `if (type(resp) is str or type(resp) is unicode)`

修改为 `if (type(resp) is str or type(resp) is str)`

图 3 亲测 Sublist3r 搜索域名效果图

三、其他子域名挖掘工具

这里简单介绍一下 Aquatone 和 Amass 工具作为拓展，他们和 Sublist3r 工作原理类似，功能比 Sublist3r 更加丰富，但是速度上却慢的多。

1. Aquatone

Aquatone 是由 go 语言、node.js 编写的子域名搜索程序，分为 4 个功能，具体如下：1）aquatone-discover：使用被动收集或字典爆破方式发现子域名；2）aquatone-scan：完成子域名扫描后，可扫描域名开放端口、HTTP header、HTML body、截图等信息并生成报告；3）aquatone-gather：对扫描结果中的 IP 进行访问请求和网页截图，搜集信息；4）aquatone-takeover：检测域名是否存在子域名劫持风险。Aquatone 能够检测 25 种不同服务提供商可能存在的子域名劫持，包括 GitHub Pages, Heroku, Amazon S3, Desk 和 WPEngine。但是响应非常慢，如果对子域名的完整度没有苛刻的要求，不建议使用。

安装命令：git clone https://github.com/michenriksen/aquatone.git

gem install aquatone

使用平台：Linux/Macos

命令格式：aquatone-discover --domain example.com

注意：由于 Aquatone 使用了许多国外的 API，因此响应较慢。此外，Aquatone 使用 VirusToal、shodan、PassiveTotal 服务，这些服务会要求提供 API KEY，你需要将这些 key 保存到 ~/aquatone/.keys.yml 路径。

```
 ____ _____ ___ ______ _/ /_____ ____ ___
 / __ `/ __ `/ / / / __ `/ __/ __ \/ __ \/ _ \
/ /_/ / /_/ / /_/ / /_/ / /_/ /_/ / / / /  __/
\__,_/\__, /\__,_/\__,_/\__/\____/_/ /_/\___/
        /_/  discover v0.5.0 - by @michenriksen

Identifying nameservers for bilibili.com... Done
Using nameservers:

 - 162.14.25.248
 - 61.151.180.51

Checking for wildcard DNS... Done

Running collector: Google Transparency Report... Timed out
Running collector: Netcraft... Done (0 hosts)
Running collector: Threat Crowd... Error
 -> Threat Crowd API returned unexpected status code: 503
Running collector: Censys... Skipped
 -> Key 'censys_secret' has not been set
Running collector: Dictionary... Done (8210 hosts)
Running collector: Riddler... Skipped
 -> Key 'riddler_username' has not been set
Running collector: VirusTotal... Skipped
 -> Key 'virustotal' has not been set
Running collector: Wayback Machine... Timed out
Running collector: HackerTarget... Done (15 hosts)
Running collector: PTRArchive... Error
 -> PTRArchive returned unexpected response code: 503
Running collector: DNSDB... Done (0 hosts)
Running collector: PassiveTotal... Skipped
 -> Key 'passivetotal_key' has not been set
Running collector: Certificate Search... Done (0 hosts)
Running collector: PublicWWW... Done (0 hosts)
Running collector: Shodan... Skipped
 -> Key 'shodan' has not been set

Resolving 8215 unique hosts...
103.41.165.61   163.bilibili.com
103.41.165.30   account.bilibili.com
103.41.165.10   activity.bilibili.com
119.3.238.64    api.bilibili.com
119.3.238.64    api.live.bilibili.com
120.131.2.207   api.vc.bilibili.com
119.3.234.165   app.bilibili.com
42.159.161.152  autodiscover.bilibili.com
```

图 4 亲测 aquatone 搜索子域名效果图

2. Amass

Amass 是由 go 编写的子域名程序[6]，是个强大的信息收集工具，接入了许多第三方 API，数据来源非常多，可以参考官方文件进行配置，此外还引入了对 d3.js 的支持，可以看到良好的可视化效果，但是尽管搜索比较全面，但是速度非常慢，搜索 bilibili.com 子域需要 15 分钟（国科大网络），非必须不建议。

```
chenxudeMacBook-Pro:~ chenxustep$ amass enum -d bilibili.com
Querying Crtsh for bilibili.com subdomains
Querying Ask for bilibili.com subdomains
broadcastlv.chat.bilibili.com
chat.bilibili.com
Querying Pastebin for bilibili.com subdomains
163.bilibili.com
api.live.bilibili.com
api.vc.bilibili.com
s.search.bilibili.com
live.bilibili.com
comment.bilibili.com
security.bilibili.com
search.bilibili.com
bvpn.bilibili.com
vc.bilibili.com
api.bilibili.com
www.bilibili.com
member.bilibili.com
app.bilibili.com
game.bilibili.com
t.bilibili.com
Querying URLScan for bilibili.com subdomains
Average DNS queries performed: 1631/sec, Average retries required: 67.69%
Querying ThreatMiner for bilibili.com subdomains
tb.bilibili.com
maoer.bilibili.com
apix.bilibili.com
pictures.bilibili.com
pgame.bilibili.com
apigame.bilibili.com
```

图 5 亲测 Amass 搜索子域名效果图

官方文档：https://github.com/OWASP/Amass/blob/master/doc/user_guide.md

使用平台：Linux/Macos

命令格式： amass enum -d example.com

安装：macos： brew tap caffix/amass

brew install amass

Linux： sudo snap install amass

四、参考资料

[1]https://www.freebuf.com/sectool/183959.html

[2]https://www.seoxiehui.cn/article-51007-1.html

[3]https://blog.csdn.net/weixin_43605586/article/details/103366043?utm_medium=distribute.pc_relevant.none-task-blog-BlogCommendFromMachineLearnPai2-2.channel_param&depth_1-utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromMachineLearnPai2-2.channel_param

[4] http://www.tt44.com/keji/172840.html

[5]https://www.jianshu.com/p/64f95a4fae5a

[6]https://www.cnblogs.com/ax-y/p/13299998.html