本文将详细介绍subDomainsBrute,来自李劼杰的博客。

### subDomainsBrute特点

用小字典递归地发现三级域名，四级域名、五级域名等不容易被探测到的域名

字典较为全面，小字典就包括3万多条，大字典多达8万条

默认使用114DNS、百度DNS、阿里DNS这几个快速又可靠的公共DNS进行查询，可随时修改配置文件添加你认为可靠的DNS服务器

自动筛选泛解析的域名，当前规则是： 超过10个域名指向同一IP，则此后发现的其他指向该IP的域名将被丢弃

整体速度还过得去，在我的PC上，每秒稳定扫描100到200个域名（10个线程）

### subDomainsBrute安装及使用使用

1、首先你必须要有一个python环境，没有的这里下载，推荐使用python 2.7.10

[https://www.python.org/downloads/release/python-2710/](https://www.python.org/downloads/release/python-2710/" \o "https://www.python.org/downloads/release/python-2710/" \t "http://www.waitalone.cn/_blank)

2、下载subDomainsBrute到本地，下载地址在下面：

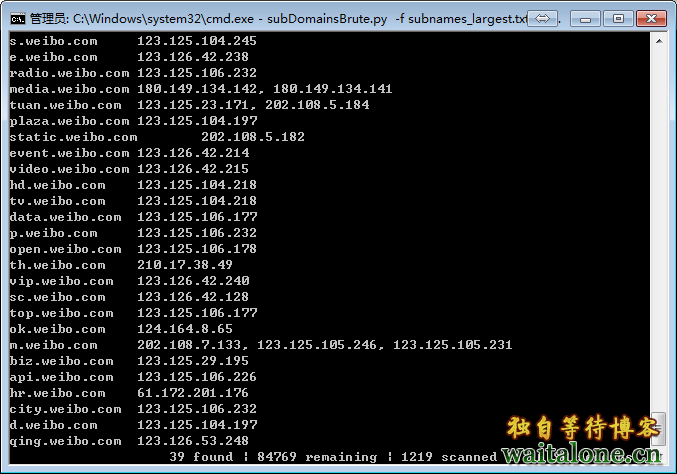
[git下载](https://github.com/lijiejie/subDomainsBrute" \o "git下载" \t "http://www.waitalone.cn/_blank) [百度网盘](http://pan.baidu.com/s/1dDGvXqp" \o "百度网盘" \t "http://www.waitalone.cn/_blank)

3、安装所需要的库，直接使用pip安装，如下：

**pip install dnspython**

4、开始使用吧，如下图：

subDomainsBrute.py waitalone.cn



原文地址：http://www.lijiejie.com/subdomainsbrute-python-script/