

隐藏源 IP，提高溯源难度的几种方案 – FreeBuf 网络安全行业门户

本文目标读者是对网络攻防技术、网络安全技术感兴趣的相关读者，可以将本篇文章作为一个思路上的启发科普文章。切记遵纪守法，交流技术！网络不是法外之地！

为什么会有此文：

原因一：保护个人隐私是是第一出发点；科技进步飞快，网络也渗透入生活中的方方面面，近几年的隐私泄露事故时有发生，我们该如何保护个人隐私？

原因二：得到了大佬的帮助和指点，希望把对我的指点内容记录一下，也能为其他人提供一点点帮助！

测试方式：

通过 CS4.2 生成测试程序，测试回连 C2 服务器时能否达到隐藏服务器的 IP

公网服务器真实 IP：1.2.3.4

Cobalt Strike 版本：4.2

所有需要注册帐号的步骤，都建议使用自己安全的邮箱！

一、使用隧道转发进行代理

一句话核心原理：利用内网穿透，将 C2 回连端口映射到其他公网地址 64.x.x.x，以达到测试程序通过其他公网地址进行回连，隐藏 C2 真实 ip；





方案分析：

适合用户：这种隐藏 ip 的方案适合于没有公网服务器，使用自己本地电脑进行测试的用户；或者有公网服务器，通过本方案隐藏服务器真实 ip 的用户；

优点：免费使用他人提供的隧道服务，可以快速的用来测试，0 成本；

缺点：使用了他人提供的隧道服务 (增加了风险)；且注册账号时还需要完成微信绑定 (增加了风险)；国内平台 (增加了风险)；

使用流程：

1. 打开网站

<https://www.ngrok.cc/> 注册 ngrok 账号

欢迎注册 Sunny-Ngrok

创建一个新账户

请输入电子邮箱

请输入用户名

请输入密码

请再次输入密码

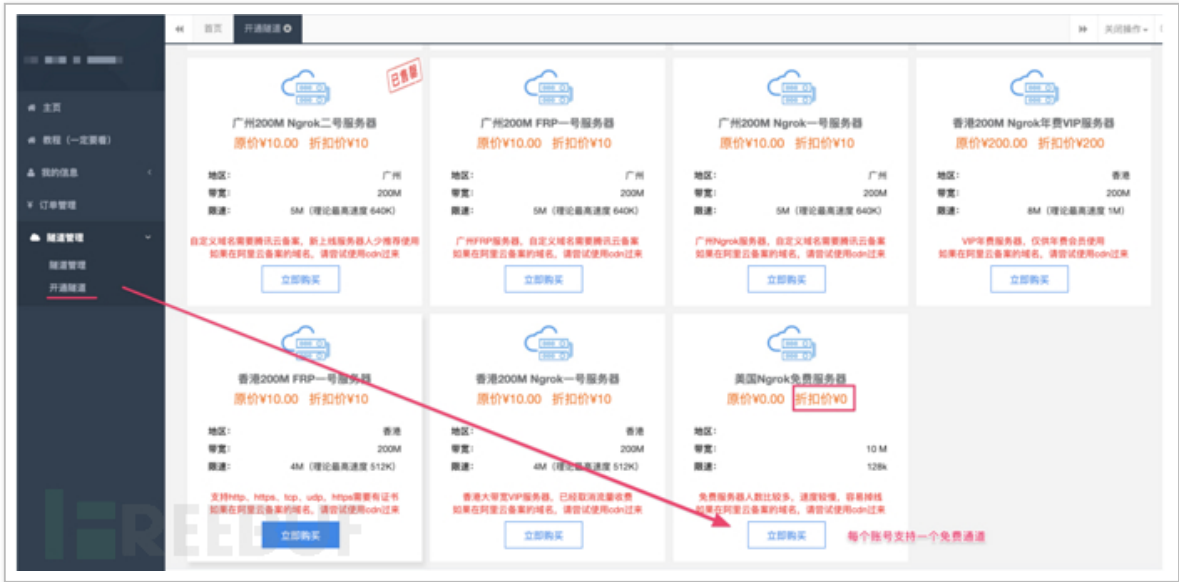
验证码

注册



2. 登录后配置 ngrok 代理

2.1 购买一个免费通道



2.2 配置通道

隧道类型分为 http、https、tcp

我们本次测试 tcp 通道，http、https 各位有兴趣的自己尝试；



因为映射到公网的远程端口有限，所以我们需要多次查询可用的远程端口，例如：

查询到 10001 端口可用 那就选择 tcp 端口映射 公网服务器的 10001 端口 <---

--- 映射 ----> 本地 127.0.0.1:8080 端口

隧道协议: tcp

隧道名称: tcp-test

远程端口: 10001
①TCP访问端口, 请输入1024-65534的端口

本地端口: 127.0.0.1:8080
①本地映射端口, 如需修改其他端口, 则输入 127.0.0.1:8000

确定开通 返回选择服务器

最终配置如下，其中隧道 ID 就是我们后面要用到的；隧道域名就是对外部公网提供访问时的公网域名；



3. 穿透工具使用说明 https://www.ngrok.cc/_book/

3.1 下载可执行程序 <https://www.ngrok.cc/download.html>



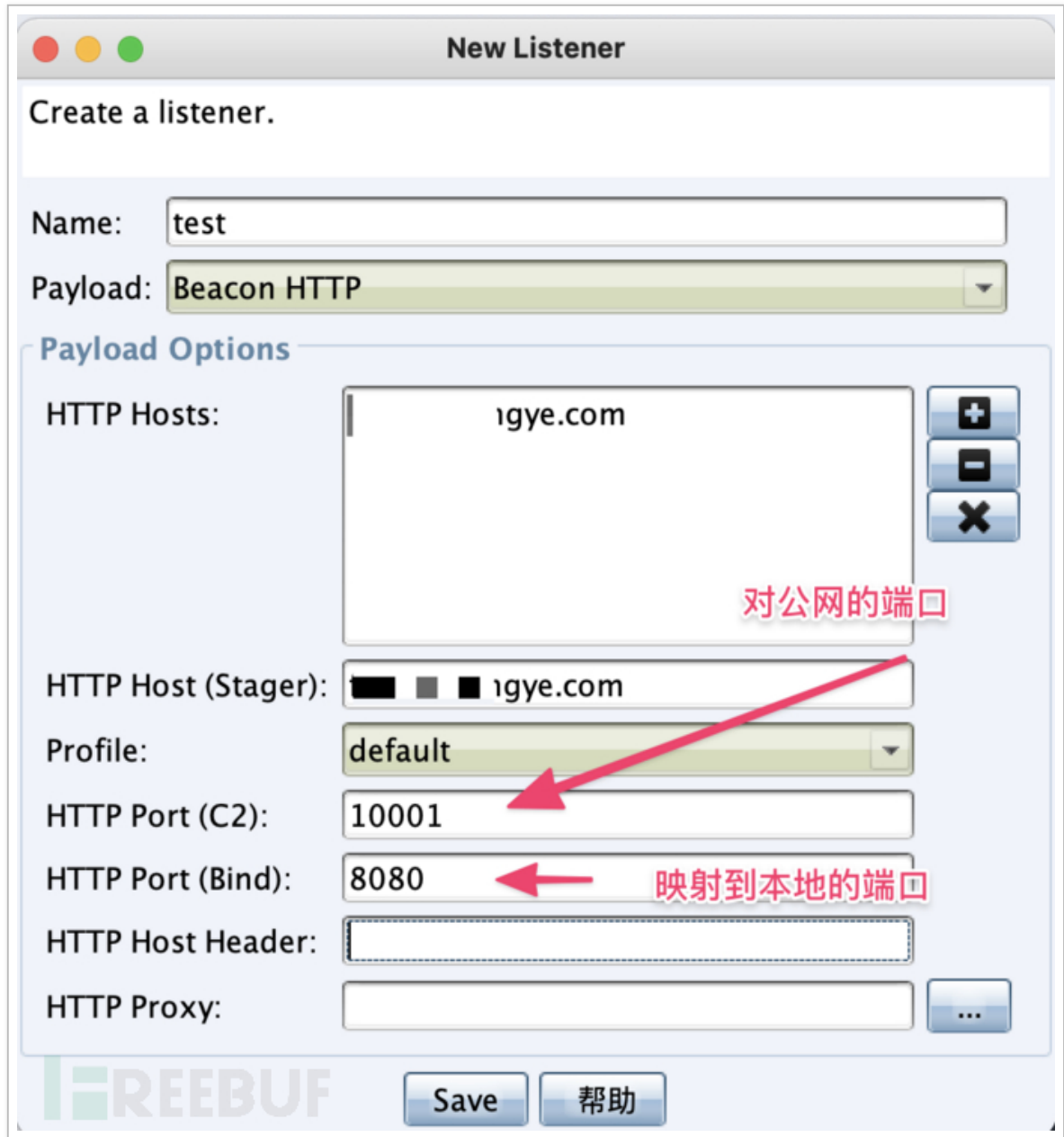
3.2 运行隧道穿透

```
#./sunny clientid 45e3634aAAAAAAAAAAAA #隧道id
```



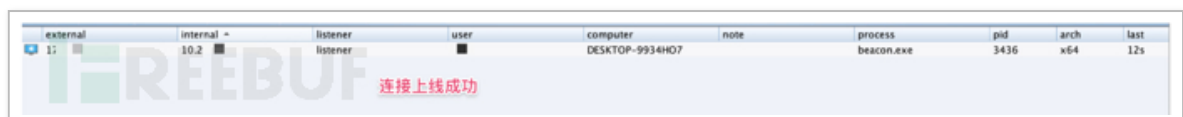
运行成功后，所有访问 xxx.xxxxxgye.com:10001 会和本地 8080 端口打通透明传输；

4. 配置 listener



5. 生成 payload，运行测试

5.1 运行 payload，主机可以成功上线；



5.2 查看本地回接 C2 服务器的 ip 地址为

xxx.xxxxxgye.com:10001(67.x.x.x:1001); 而不是我们自己服务器的真实 ip!

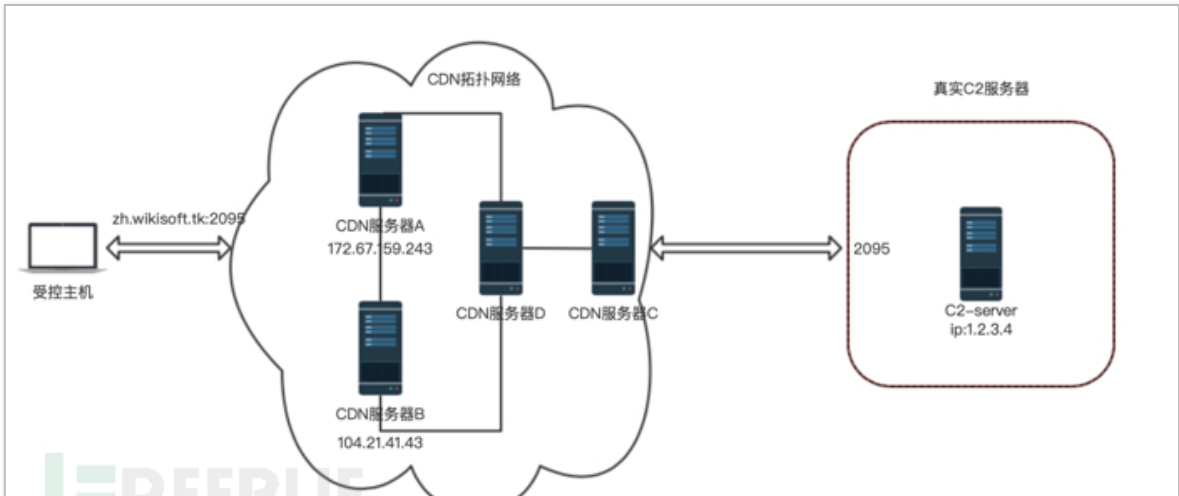


上面的 64.X.X.X 就是 ngrok 的公网 ip

搞定！

二、使用 CDN

一句话核心原理：使用 CDN 内容分发网络的多节点分布式技术，通过“加速、代理、缓存”隐藏在后面的静态文件或服务；最终实现对外暴露的是 CDN 多节点的公网域名 IP，很难甚至无法溯源真实后端服务器的域名或 IP！



方案分析：

适合用户：这种隐藏 ip 的方案适合于有公网服务器，通过本方案 CDN 进行“加速、代理、缓存”实现隐藏服务器真实 ip 或域名的用户；使用国内 CDN 服务商的产品的域名必须完成 ICP 实名备案；

优点：利用 CDN 分布式技术，不同区域的主机就近连接到 CDN 服务，优化了访问质量，隐藏了真实服务器的 ip；且 CDN 分布式技术可以在一定程度抵抗 DDOS 大流量攻击；使用国内 CDN 适合用于做红蓝对抗技术比拼等合法目的；

缺点：受控主机还是通过我们自己的域名进行回连，对外还是能看到连接域名；且如果使用国内 CDN 的服务（增加了风险），域名就必须完成 ICP 备案（增加了风险）；而且还有一些方法可能溯源到真实 IP（请一定要按照下面的参考文章 1、2，进行子查一下！）；

使用流程：

（匿名注册新域名且无需备案 + 使用国外免费 CDN 服务）

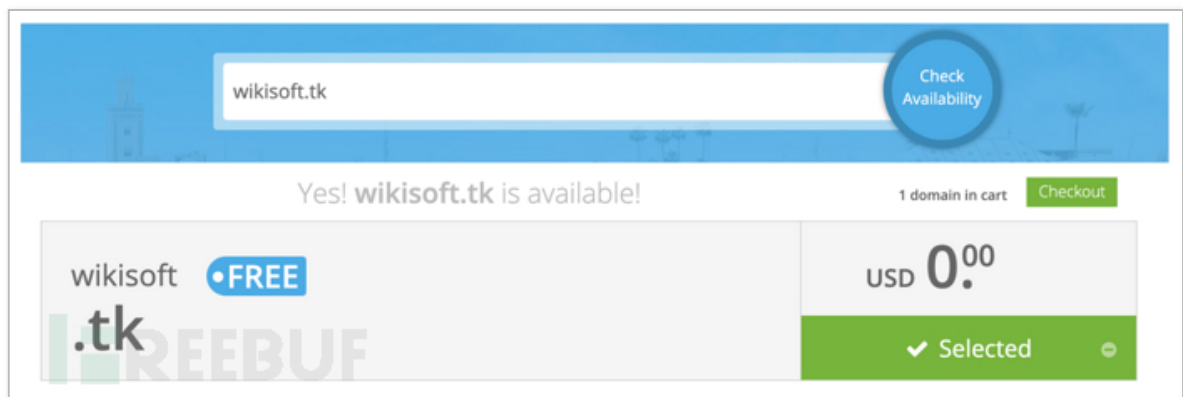
1. 匿名注册新域名：

<https://www.freenom.com/zh/index.html?lang=zh>

1.1 完成账号注册登录（注册可以先不做，继续选域名后面会有一个步骤让我们注册账号）；

1.2 搜索域名：

小坑提醒：这里有一个坑，搜索 wikisoft, 会显示所有域名不可用；但是搜索 wikisoft.tk 就可以；所以一定要搜索域名全称！



1.3 下单确认：

Review & Checkout

Description	Price
Domain Registration - wikisoft.tk	\$0.00USD
Subtotal:	\$0.00USD
Total Due Today:	\$0.00USD



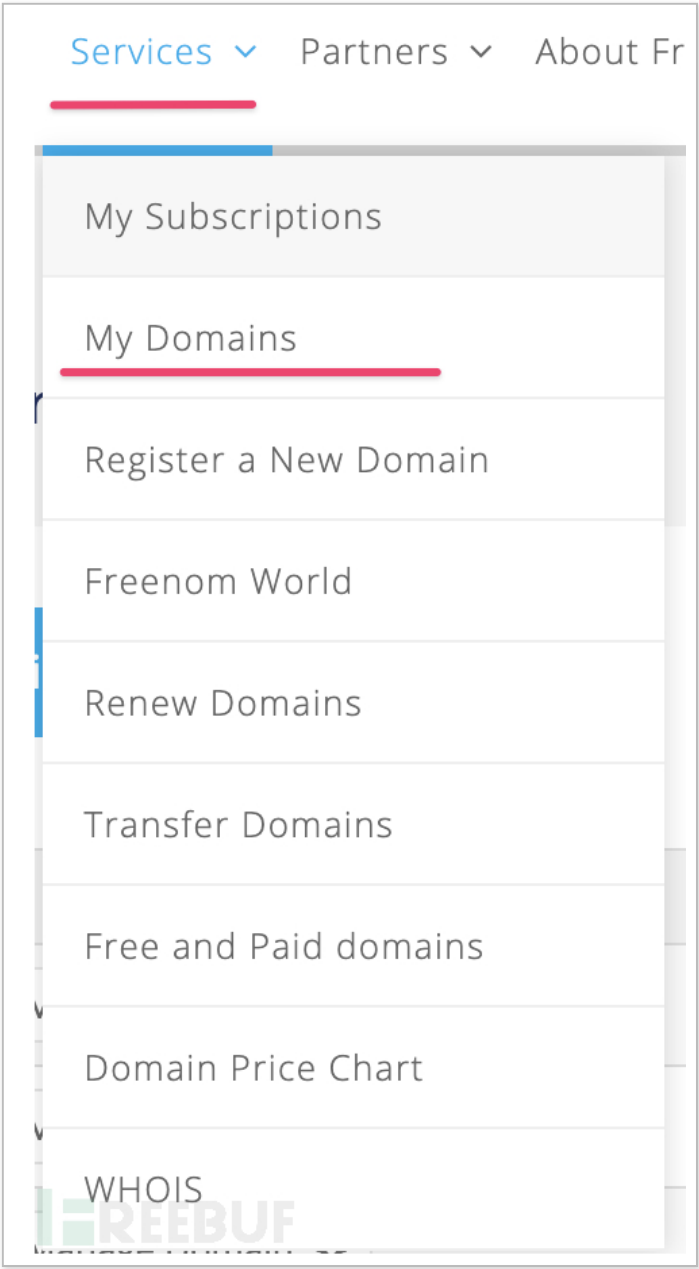
☒ I have read and agree to the Terms & Conditions

Complete Order

如果之前没有注册过域名，点击“继续”按钮，会让我们进行注册账号，或者验证邮箱；然后进行登录再进行选购域名；（这里如果注册失败，可以用 gmail 注册。）

1.4 配置域名的 NameServer 域名解析服务（这样做，后面再解释为什么；现在不修改，默认配置，也可以后面再修改）

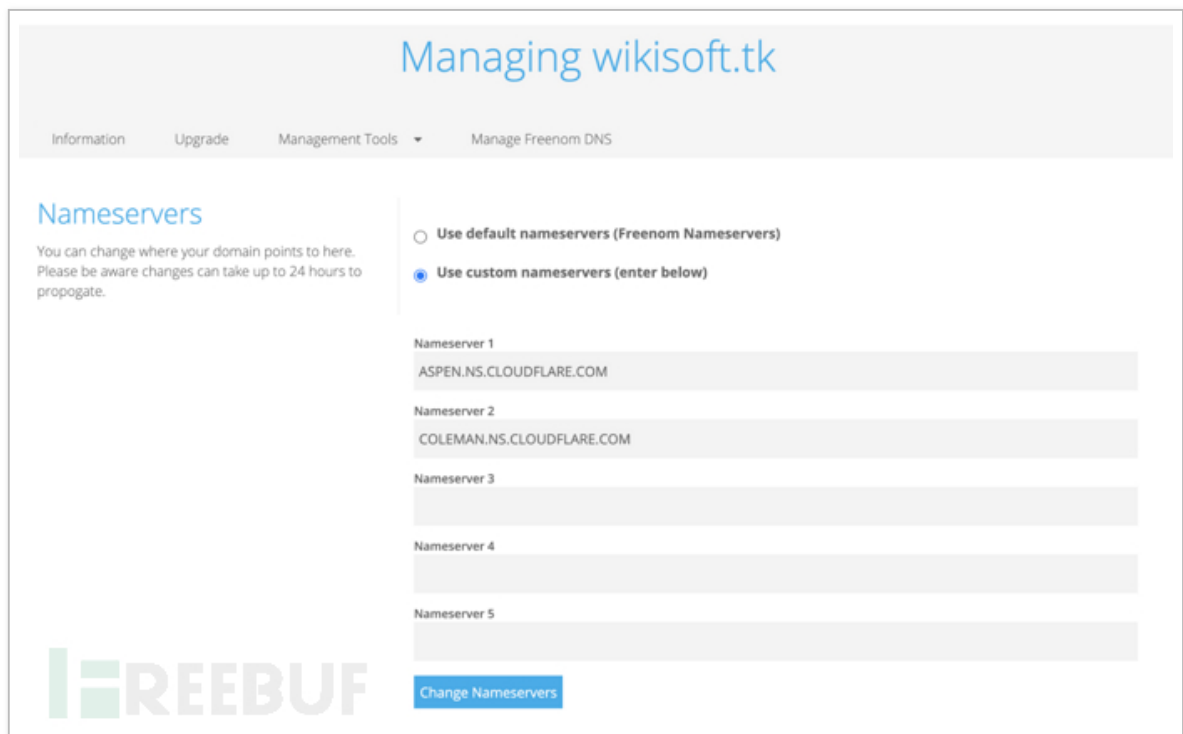
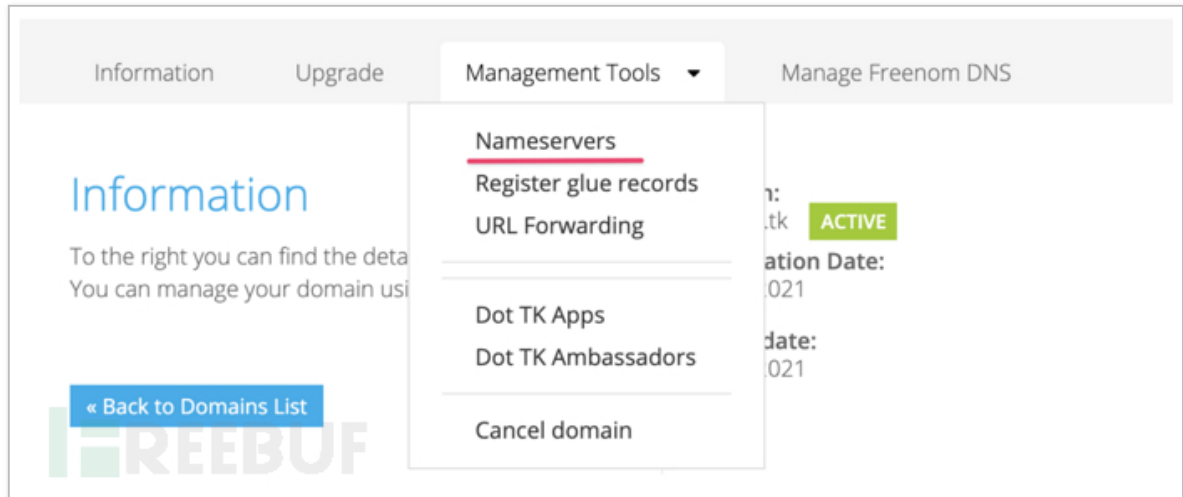
1.4.1 进入我的域名：



1.4.2 选择域名管理：

Domain	Registration Date	Expiry date	Status	Type	
wikisoft.tk	2021-04-23	2021-07-23	ACTIVE	Free	Manage Domain

1.4.3 选择域名解析服务进行修改



ASPEN.NS.CLOUDFLARE.COM COLEMAN.NS.CLOUDFLARE.COM

匿名域名注册及配置完毕！

2. 匿名注册免费 CDN 服务 Cloudflare

2.1 登录注册账号 <https://www.cloudflare.com/zh-cn/>

2.2 配置域名使用 CDN

2.2.1 添加站点

借助 Cloudflare 加速和保护您的站点

输入您的站点 (example.com):

想要添加多个站点? [了解方法。](#)

2.2.3 选择免费计划

1 选择您的计划

2 查看 DNS 记录

3 更改您的名称服务器

选择计划

Pro

US\$20/月

按月计费

面向专业人员的 Cloudflare 适用于希望保护其专业网站或博客安全并加快其专业网站或博客运行速度的用户。

核心功能

Free 计划中的全部功能，以及：

增强型 Web 应用程序防火墙 (WAF) 安全性

无损图像优化

自动移动优化

缓存分析

支持资源：平均电子邮件响应时间：小于 4 小时。

Business

US\$200/月

按月计费

Cloudflare PCI 合规 Business 计划适用于在线运营的小型业务。此软件包可提供 100% 运行时间 SLA 以及各种高级安全功能，并且可以为用户提供优先客户支持服务。

核心功能

Pro 计划中的全部功能，以及：

全年全天候支持

100% 运行时间 SLA

CNAME 设置兼容性

简易 PCI 合规性

使用自有 SSL 证书

支持资源：平均电子邮件响应时间：小于 2 小时。

Enterprise

联系我们

请填写此联系表，然后选择 Free 计划继续。

面向需要企业级安全性和性能、优先的 24/7/365 电话、电子邮件或聊天支持，以及有保障的运行时间的公司。

核心功能

Business 计划中的全部功能，以及：

优先 IP 范围

指定解决方案工程师支持

25 倍赔偿运行时间 SLA

基于角色的帐户访问

支持资源：平均电子邮件响应时间：小于 1 小时。

不知道从哪里开始？
免费开始使用。

Free

0 美元

面向个人的 Cloudflare 是基于我们的全球网络开发的。此软件包适用于从事非业务关键型个人或业余项目的用户。

核心功能：
DDoS 攻击缓解
全球内容分发网络
电子邮件支持

哪个计划适合您？ [了解更多。](#)

继续

2.2.4 直接配置使用 CDN 代理模式进行域名解析提供服务

上面 1.4，配置 NameServer 更换解析服务器的原因就是，将 wikisoft.tk 域名的所有解析功能都托管在 Cloudflare，这样 Cloudflare 可以提供 CDN 的解析功能！

为 wikisoft.tk 添加更多 DNS 记录

单击云形图标来代理 A、AAAA 和 CNAME 记录的流量。

 已代理：加速和保护流量

 仅 DNS 解析：绕过 Cloudflare

注意：不带云形图标的记录将使用 DNS 解析，但是不能被代理。

管理 wikisoft.tk 的 DNS

+ 添加记录

Q 搜索 DNS 记录

≡ 高级

zh.wikisoft.tk 指向 1.2.3.4 并通过 Cloudflare 代理其流量。

类型

名称

IPv4 地址

TTL

代理状态

A

zh

1.2.3.4

自动

 已代理

换成你自己公网服务器的 ip

取消

保存

类型	名称	内容	TTL	代理状态
----	----	----	-----	------

继续

FREEBUF

2.2.5 自动配置全部选择关闭

[← 返回](#)

快速入门指南

配置域设置以提高安全性、优化性能并充分利用帐户。

- 1 提高安全性
- 2 优化性能
- 3 摘要

自动 HTTPS 重写: **OFF**

始终使用 HTTPS: **OFF**

Auto Minify: **NONE**

Brotli: **OFF**

[完成](#)



2.2.6 配置 SSL/TLS 加密方式 (默认不加密, 有兴趣的自己尝试其他加密的区别)



注意：Cloudflare 的 CDNhttp、https 代理模式有个特点，如果用其他端口的话，是监听不到的！

因为我是使用的国内云主机，且 zh.wikisoft.tk 没有进行备案，所以没有办法使用 80、8080、443、8443 端口提供服务；所以我真实云主机的回连端口使用的是 http--2095！如果你用的是国外云主机，那就直接用 80！

Cloudflare支持的HTTP端口是： 80,8080,8880,2052,2082,2086,2095 Cloudflare支持的HTT
Ps端口是： 443,2053,2083,2087,2096,8443

到此域名 + CDN 全部搞定！开始测试！

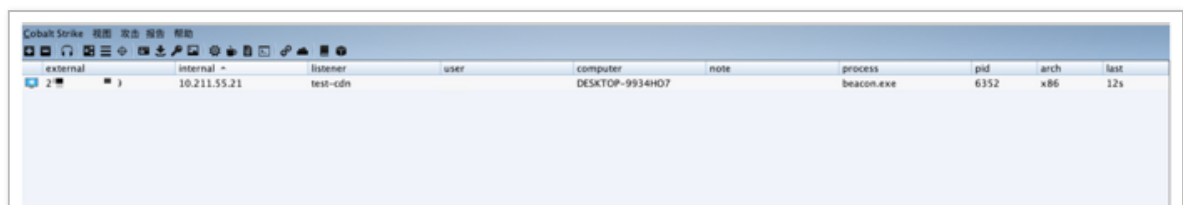
3. 配置 listener

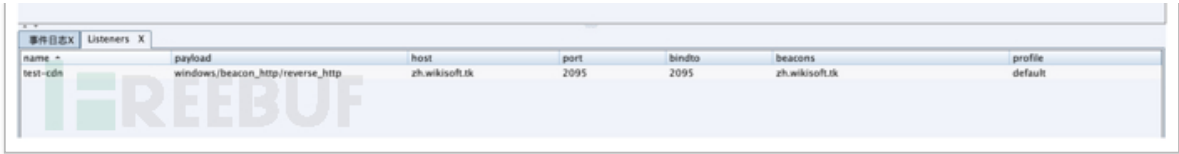
HTTP Host Header，必须填写你的域名！这是 CDN 技术的原理要求；在下面的“域名前置方”案中我们再解释



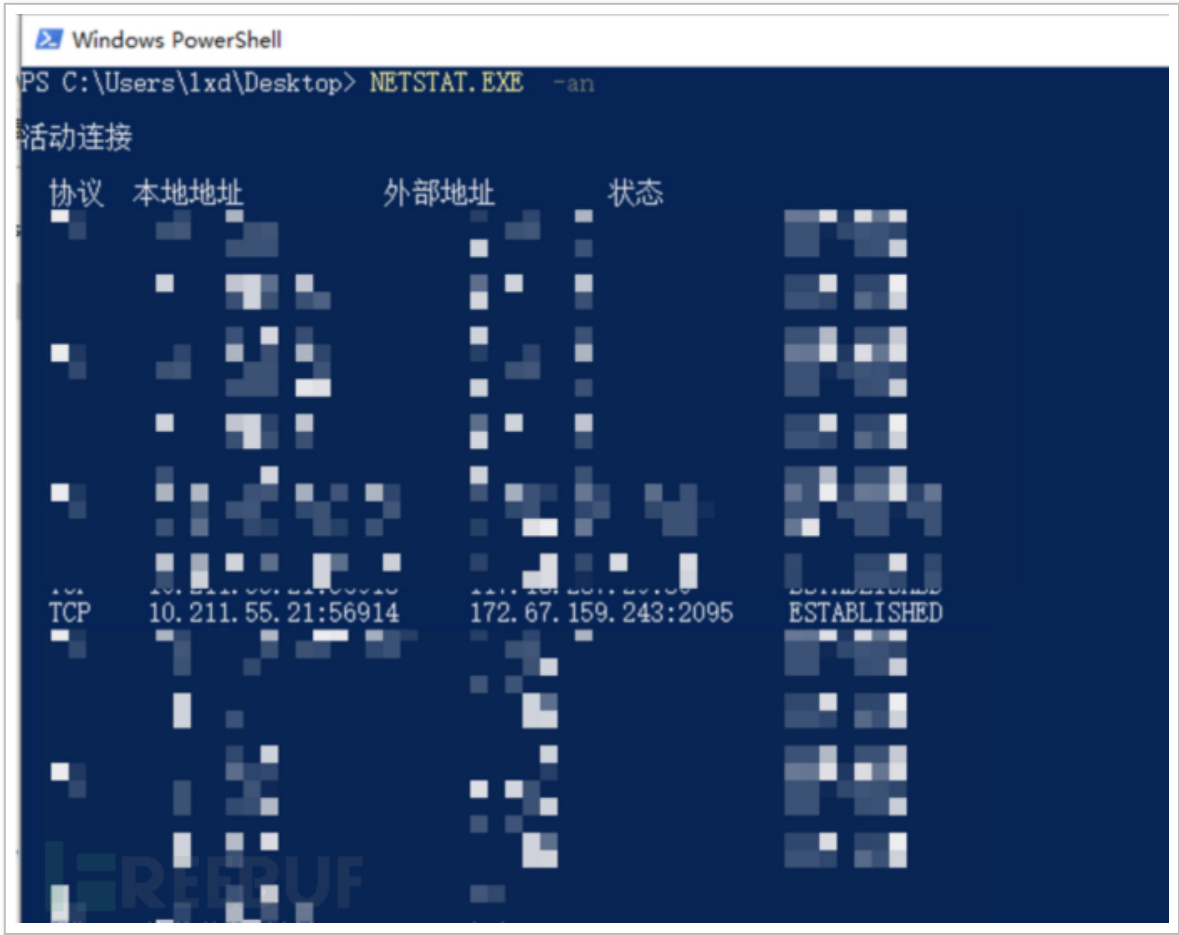
4. 生成 payload，运行测试

4.1 运行 payload，主机可以成功上线；





4.2 查看受控主机本地回接 C2 服务器的 ip 地址为 172.67.159.243:2095（CDN 节点 ip）；而不是我们自己服务器的真实 ip



4.3 再来说一下这个 ip 是啥：这个 ip 就是我们使用的 Cloudflare 的最近 CDN 节点的公网 ip

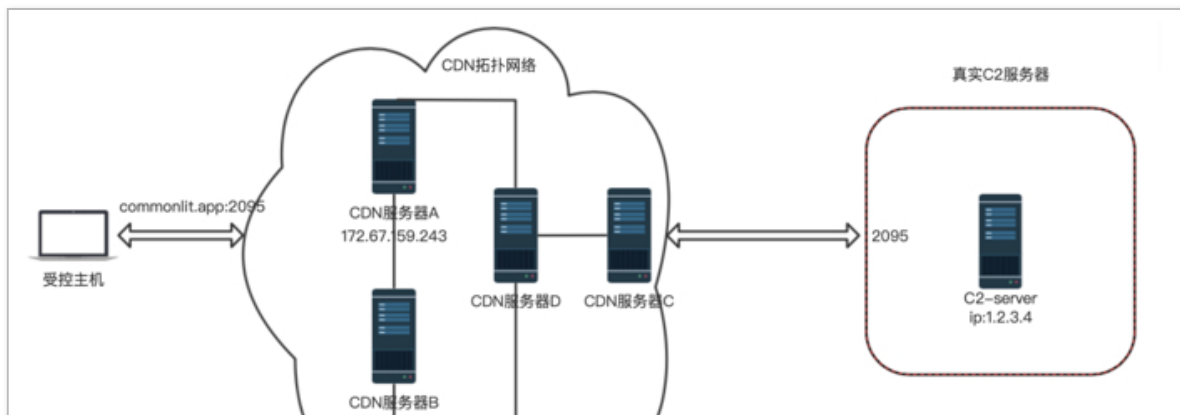
```
➤ Desktop nslookup zh.wikisoft.tk
Server:                223.5.5.5
Address:               223.5.5.5#53

Non-authoritative answer:
Name:   zh.wikisoft.tk
Address: 104.21.41.43
Name:   zh.wikisoft.tk
Address: 172.67.159.243
```

搞定！

三、使用域名前置 (Domain Fronting)

一句话核心原理：底层技术还是上面的 CDN，但是我们使用了其他正规可靠的域名进行连接（比如：www.baidu.com），通过设置 HOST=zh.wikisoft.tk 修改 host 头的原理，让 CDN 将连接指向我们期望的 C2 服务器；最终实现受控主机通过回连！如果使用 https 的话，除非逆向程序获取 host 头信息，否则无法获取到真实连接域名！





方案分析：

适合用户：这种隐藏域名及 ip 的方案适合于有公网服务器

优点：本方案使用高信誉域名进行连接，通常安全设备很难检测，也很难封堵；

缺点：配置和准备条件较多步骤比较复杂；如果能利用好上面的域名 + CDN 也挺好。

使用流程：

小坑提醒：我尝试使用 http 域名前置进行原理演示，因为 Cloudflare 免费版 CDN 不支持上传自定义 ssl 网站证书，只能升级成企业版才可以实现 https! (如果你是企业版，就是通过修改上面的“2.2.6 配置 SSL/TLS 加密方式”这一节就能完成 https 通的联通及域名前置！可需要申请域名的 https 证书，现在各种云平台都有一年免费证书可用，方法“参考文章 4、5”。)

1. 完成上面域名 + CDN 的所有配置

2. 获取其他也托管在 Cloudflare 并使用 CDN 的合法域名 (比如: commonlit.app)

The screenshot displays a web browser window with the URL `x.threatbook.cn/v5/p/104.21.41.43`. The page shows a domain resolution tool interface. A red arrow points to the "验证一下域名是否可用" (Verify if the domain is available) button. Below the button is a table of domain resolutions.

解析域名	域名发现时间	操作步骤	操作标签	解析IP
commonlit.app	2018-05-21	未知	暂无	172.67.159.243, 104.21.41.43
www.commonlit.app	2018-05-21	未知	暂无	172.67.159.243, 104.21.41.43
deepak.app	2019-04-01	未知	暂无	172.67.159.243, 104.21.41.43
about.deepak.app	2020-09-27	未知	暂无	-
links.deepak.app	2020-09-27	未知	暂无	-
www.deepak.app	2019-04-01	未知	暂无	172.67.159.243, 104.21.41.43
xp5.app	2020-10-04	未知	暂无	172.67.159.243, 104.21.41.43
www.xp5.app	2020-10-04	未知	暂无	172.67.159.243, 104.21.41.43
cryptobioys.com.ar	2020-04-02	未知	暂无	172.67.159.243, 104.21.41.43
www.cryptobioys.com.ar	2020-04-02	未知	暂无	172.67.159.243, 104.21.41.43

To the right of the browser window is a terminal window showing the following commands and output:

```
Last login: Fri Apr 23 11:26:44 on ttys005
➥ Desktop macosapp commonlit.app
Server: 223.5.5.5
Address: 223.5.5.5#53

Non-authoritative answer:
Name: commonlit.app
Address: 172.67.159.243
Name: commonlit.app
Address: 104.21.41.43

➥ Desktop ping commonlit.app
PING commonlit.app (172.67.159.243): 56 data bytes
Request timeout for icmp_seq 0
64 bytes from 172.67.159.243: icmp_seq=1 ttl=58 time=248.746 ms
<C
--- commonlit.app ping statistics ---
2 packets transmitted, 1 packets received, 50.0% packet loss
round-trip min/avg/max/stddev = 248.746/248.746/248.746/0.000 ms
➥ Desktop
```

3. 配置 listener

HTTP Host Header 必须填写你的域名 zh.wikisoft.tk 这是 CDN 技术的原理要

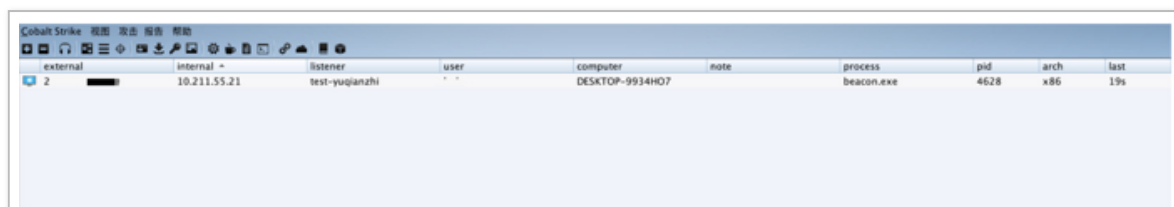
利用 Host Header，必须参与你的域名 zh.wikisoft.tk，这是 CDN 又不显示明文

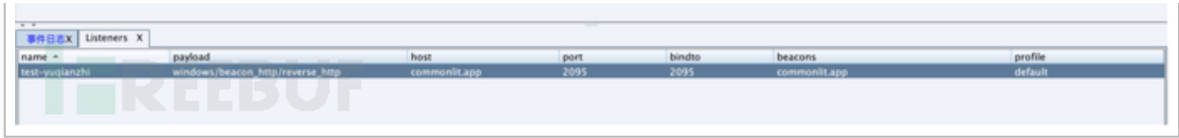
求；CDN 的 ip 都一样，如何判断用户访问的时候 baidu 还是 qq 呢？实际上就是通过 http 头里面的 host 字段进行判断的！详细内容学习“参考文章 6、7、8”



4. 生成 payload，运行测试

4.1 运行 payload，主机可以成功上线；

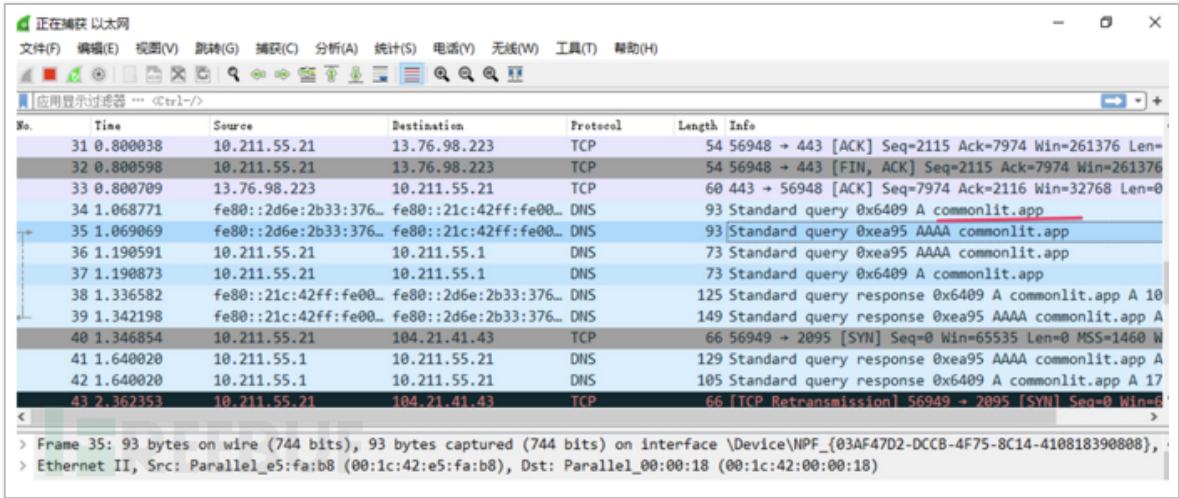




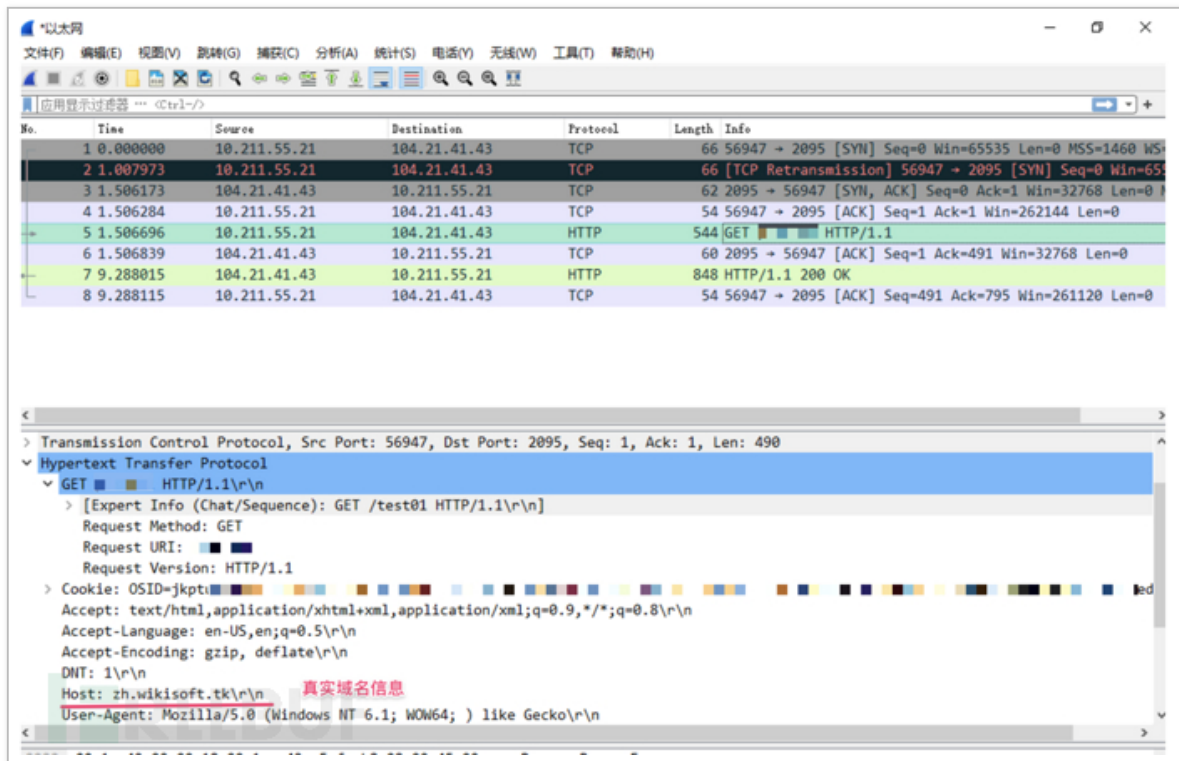
4.2 查看受控主机本地回接 C2 服务器的 ip 地址为 104.21.41.43:2095（CDN 节点 ip）；而不是我们自己服务器的真实 ip



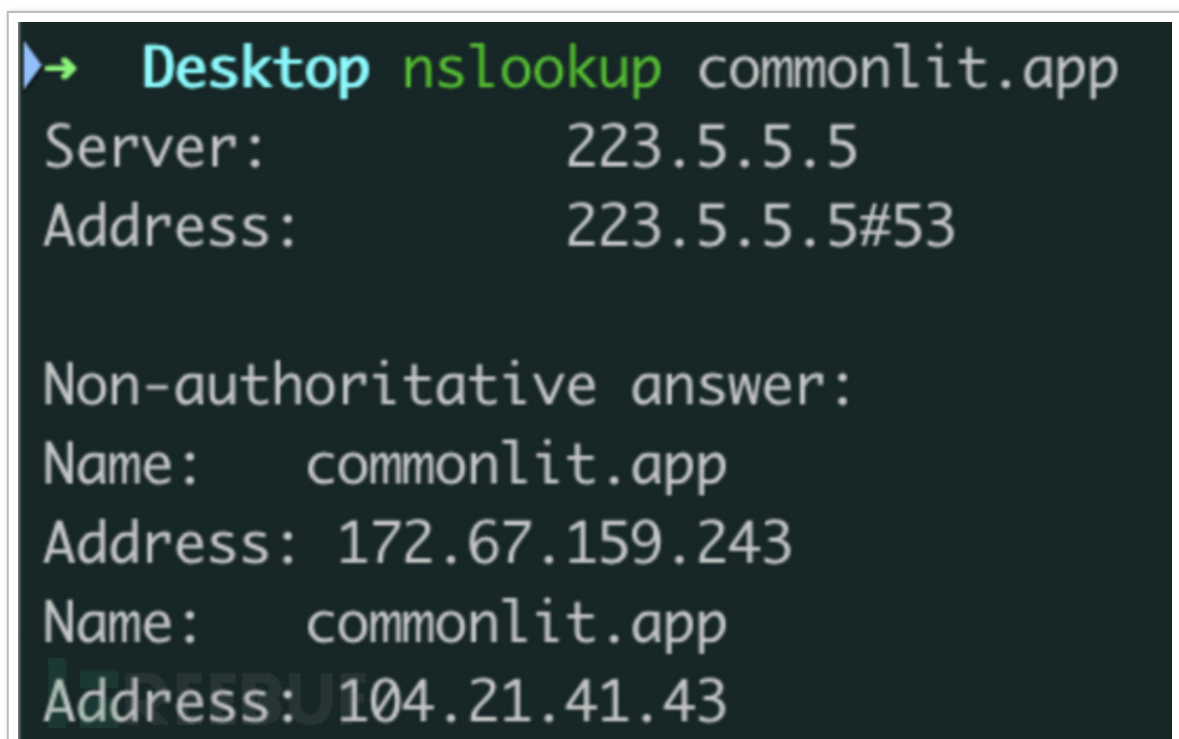
4.2.1 查看 DNS 数据包，可以确认连接过程是查询 commonlit.app:2095 这个地址，进行连接的；



4.2.2 查看连接数据包，http 方式还是可以看到 host 信息的；



4.3 再来说一下这个 ip 是啥：这个 ip 就是我们使用的 Cloudflare 的最近 CDN 节点的公网 ip

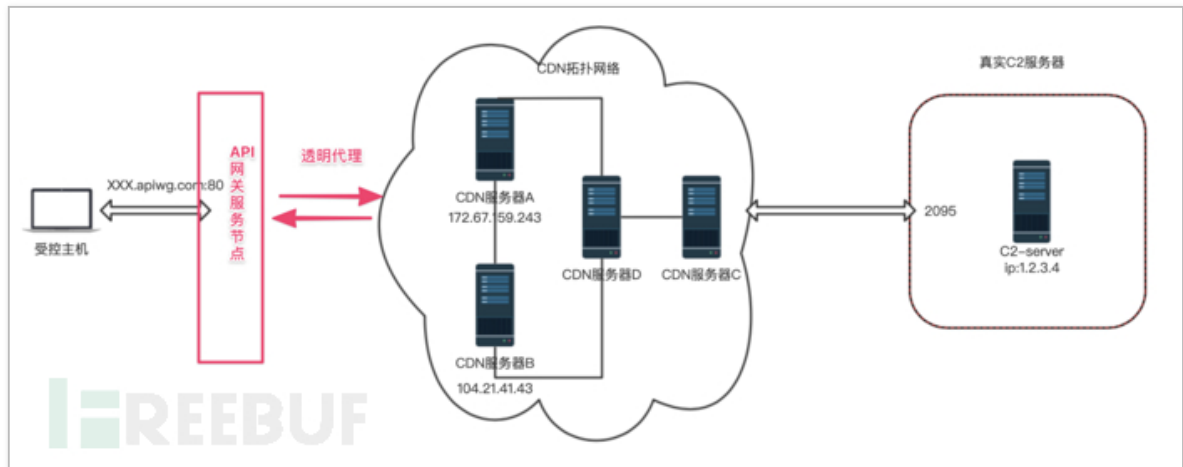


备注：使用 https 的方式进行域名前置，除非逆向程序获取 shellcode 里面的 host 内容，否则无法获取真实域名 zh.wikisoft.tk, 也无法溯源真实后端服务器的 IP！使用了 https 域名前置，就是在上面的 CDN 直接使用 zh.wikisoft.tk 域名的基础上又增加了一层安全保障！如何逆向二进制，也有教程文档“参考文章 9”

搞定！

四、使用云服务 API 网关 / 云函数

一句话核心原理：api 网关透明转发代理后端服务！（了解一 kong 网关，原理一样）；云函数底层使用的就是 api 网关，只是云函数的功能更高级一点，当 client 调用网关接口时，通过编程进行修改输入参数；同理 api 网关接受到代理的后台服务返回的内容是可以再次修改返回内容，最终将信息返回给 client；



方案分析：

适合用户：这种隐藏域名及 ip 的方案适合于有公网服务器，注册了云服务商网关或者云函数产品；

优点：本方案使用高信誉域名进行连接，通常安全设备很难检测，也很难封堵；

缺点：配置和准备条件较多步骤比较复杂；如果能利用好上面的域名 + CDN 也挺好。

使用流程：

备注：这一方案，只是原理学习，没有考虑到安全性；所以直接用了国内的云服务产品！！！各位可以自己寻找“安全”的云服务！云函数的学习“参考文章 10、11”，下面只说明底层的 api 网关内容

1. 注册 Q 云，完成相关认证

2. 配置 API 网关透明传输

2.1 新建 service



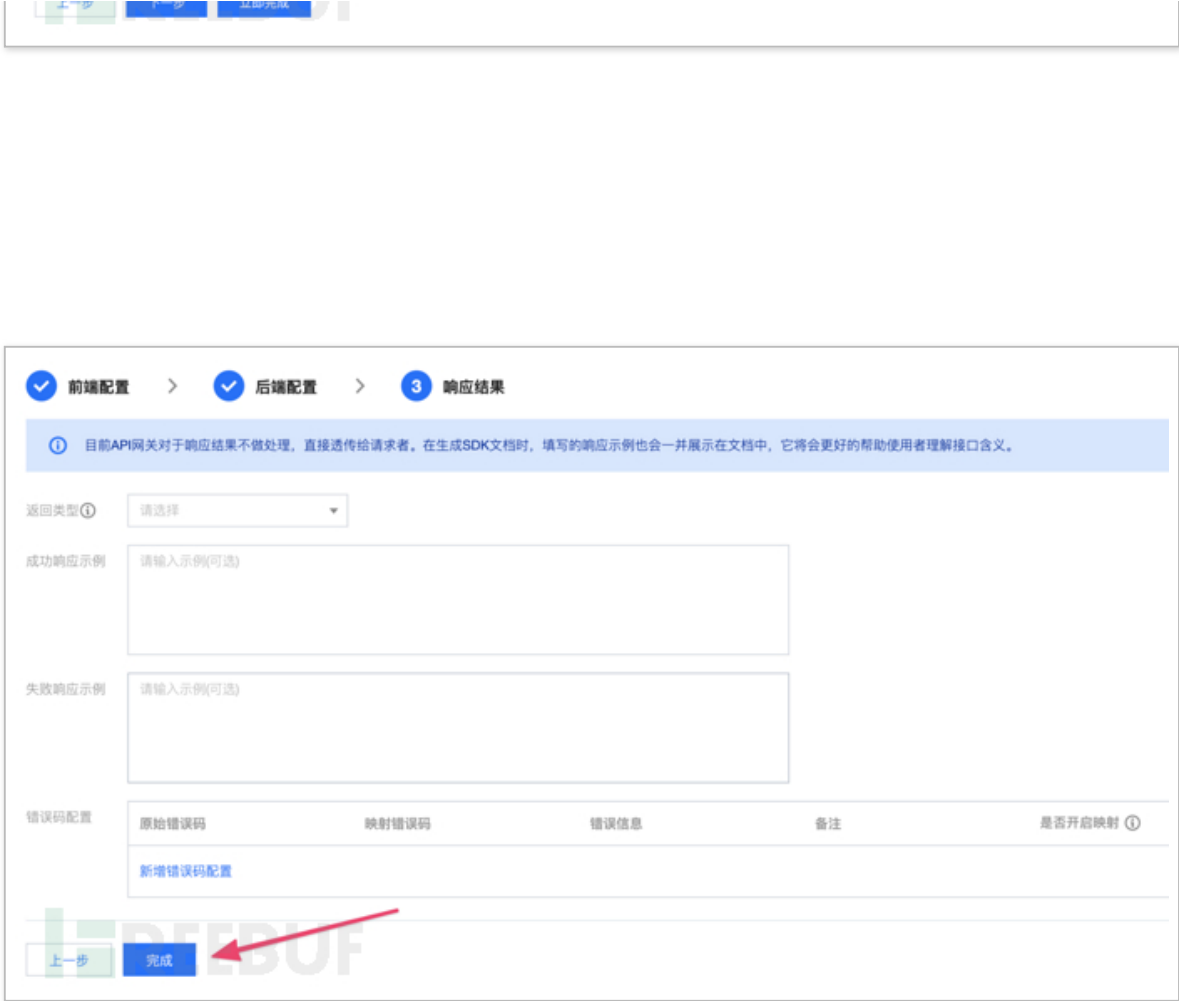
2.2 新建 API 代理并完成透明代理配置

小坑提示：前端、后端代理的超时时间都设置的长一点！以免超时！

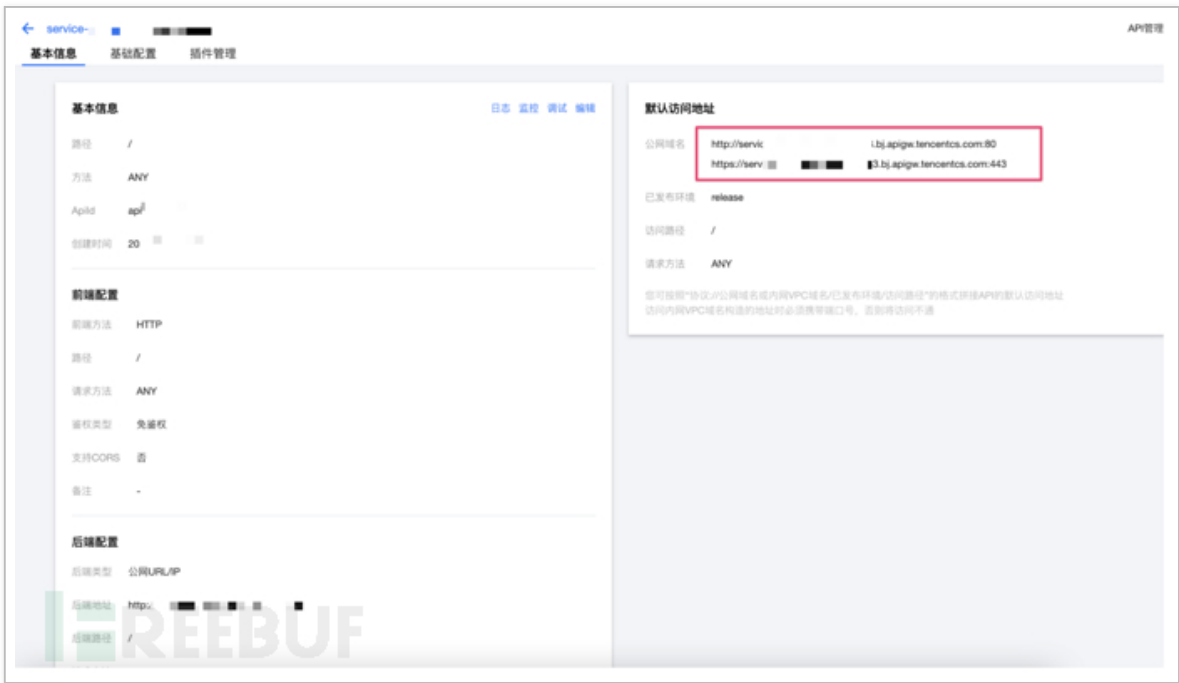


后端域名：如果是 80 端口，就直接填写域名，如果是其他端口，就写成 域名: 端口

<https://www.freebuf.com/sectool/270669.html>



2.3 查看公网接口调用地址

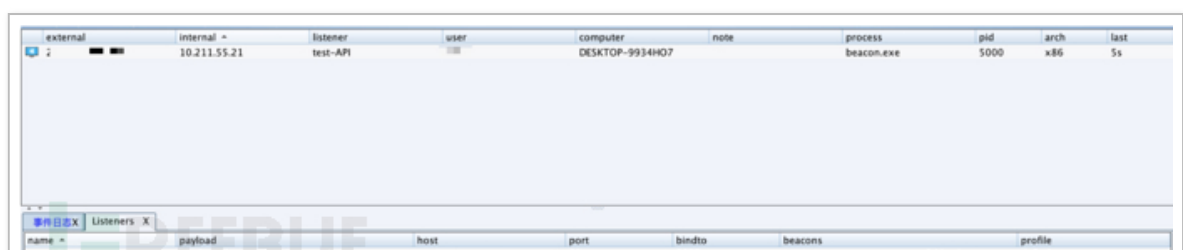


3. 配置 listener

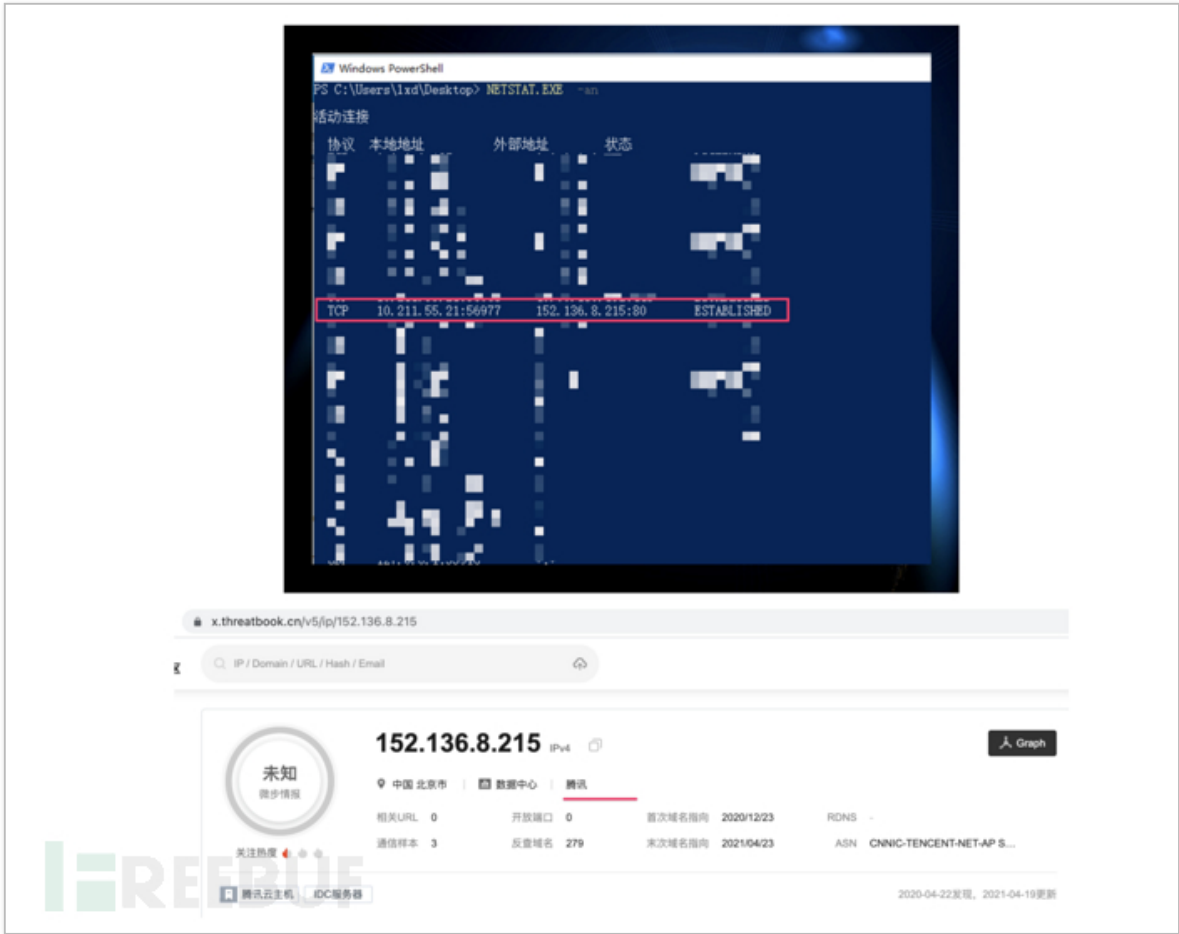


4. 生成 payload，运行测试

4.1 运行 payload，主机可以成功上线；



4.2 查看受控主机本地回接 C2 服务器的 ip 地址为 152.136.8.215:80（Q 网关节点 ip）；而不是我们自己服务器的真实 ip



搞定！！

五、再说点其他的

1. 域名直接使用 CDN 解析删除其他解析（安全分数 + 1）：既然注册了匿名免费的域名，使用目的狠命聊！那就别添加太多解析，越多维护越麻烦，泄露信息风险越大！而且，这个域名后面的所有测试过程都不要不适用代理的模式解析到 ip 或者 CNAME 到其他域名！任何历史操作都是泄露你个人信息的风险点！
2. 服务器访问 IP 源限制（安全分数 + 1）：既然使用了 CDN 服务，为了更安全，就将真实服务器防火墙 + 安全组的访问源 ip 做网段限制！设置成仅允许 Cloudflare 网段进行访问！防止其他小伙伴扫描 hack 你的 c2 服务！
3. 域名前置一定要用 https(安全分数 + 2)：使用 http 的方式玩域名前置是没意义

的，抓包就能看到 http 里面的 host 信息；而使用 https 的域名前置方式，除非二进制逆向获取 shellcode 里面的 host 信息！（这一点，， 我可能说错了，https 也能看到 host 信息~~）

4.C2 服务器安全加固（安全分数 + 1）：C2 服务器的客户端连接的 50050 端口，做好安全防护！（配置好证书确认登录指纹信息！修改其他端口避免其他网络扫描！不用的时候就防火墙安全组都 deny 或者限制登录 ip 范围！）

5. 向大佬请教 1：按照上面 CDN 的方式，注册了匿名免费域名 + 免费 CDN 服务，理论上技术手段是无法溯源到你的任何信息！除非你做了什么见不得人的事情，动用了国家力量去国外公司执法取证！！（欢迎小伙伴帮助检查一下上面的这种方式，是否可以从技术手段完成 IP 溯源，我们继续交流；）

6. 向大佬请教 2：通过国内云平台申请一年的免费 https 证书，从技术手段能通过 https 证书查到颁发机构和申请人信息吗？这个我不知道风险大小。有知道的大佬麻烦指点一下。

7. 向大佬请教 3：域名前置方案中“4.2.2”，因为我条件不具备 https，想确认一下，是否 https 的方式，就无法抓包查看 host 信息吗？（这一点，有大佬回复：https 也能看到 host 信息~~）

最后说点：感谢各位大佬的帮助和指点，这篇文章我只是替各位整理汇总了一下~_~(就不说各位的微信名称了，知道我是谁的在下面留言 call 我)！

参考文章：

1. 如何绕过 CDN 找源站 ip?
2. 如何绕过 CDN 查询网站真实 IP? 溯源方法如下
3. 反溯源 – cs 和 msf 域名上线 – 先知社区
- 4.CS 合法证书 + Powershell 上线
5. 关于合法证书 + ps 上线手把手示范
6. 【安全研究】Domain fronting 域名前置网络攻击技术
7. 域前置技术的原理与 CS 上的实现
8. 红队基础建设: 隐藏你的 C2 server
9. 新人第一次逆向 CS 生成 exe 木马
- 10.RT 又玩新套路，竟然这样隐藏 C2
11. 【技术分享】红队攻防基础建设 – C2 IP 隐匿技术
12. 关于 Cobalt Strike 的 Malleable-C2-Profiles 浅析
13. 子域名劫持 (Subdomain Takeover)

