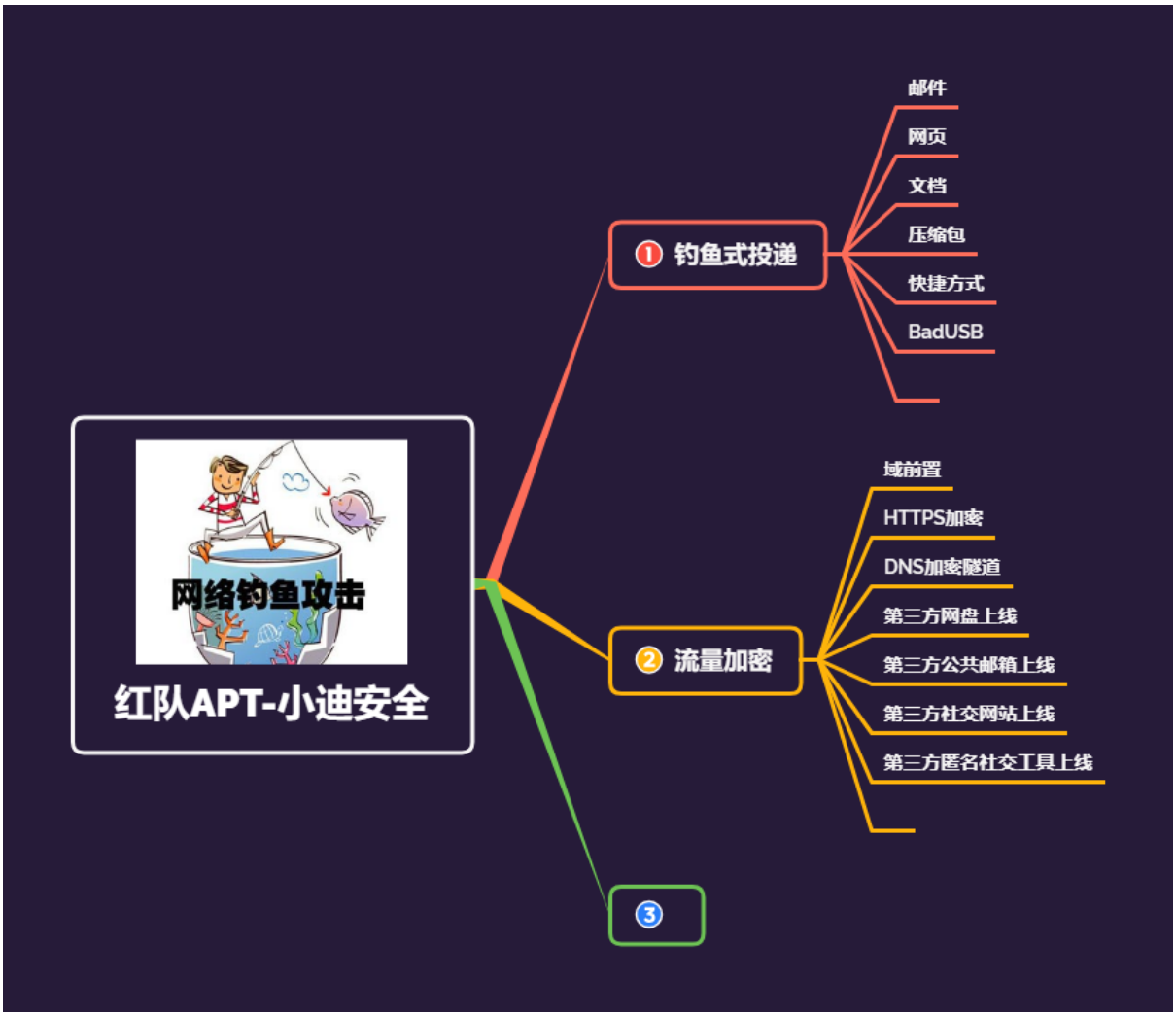
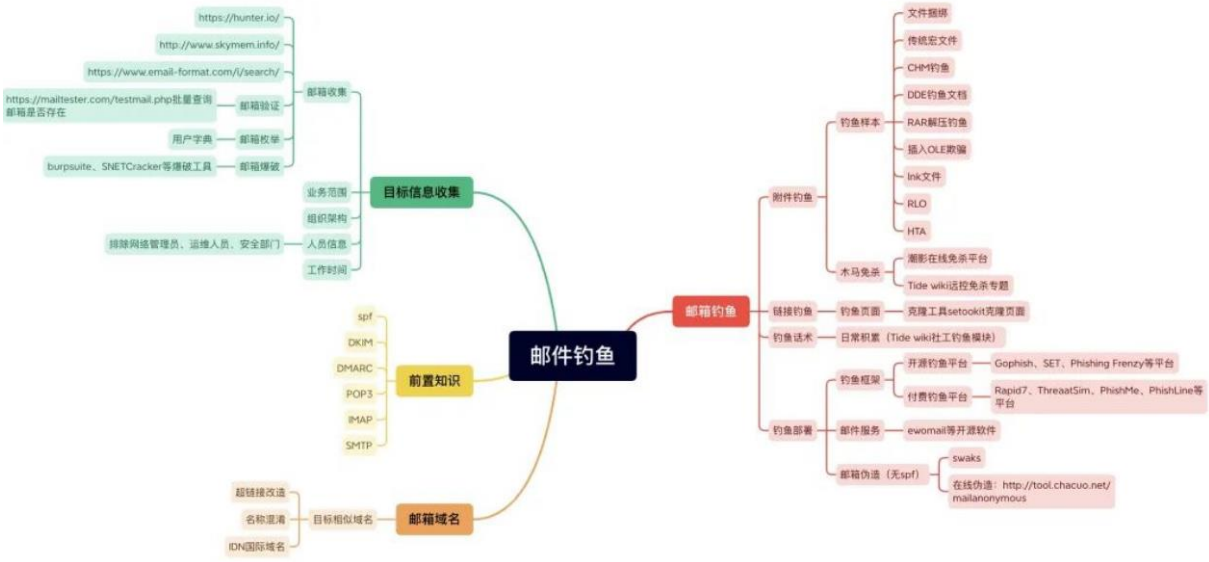
红队 APT-钓鱼篇&邮件钓鱼&Ewomail 系统&网页克隆&劫持用户&后门上线





```
#知识点：
1、红队技能-网络钓鱼-邮件系统
2、邮件钓鱼-平台-Gophish&Swaks
3、邮件钓鱼-系统-smtp2go&SendCloud
4、邮件钓鱼-自定义-Ewomail&Postfix
5、网页钓鱼-克隆修改-劫持口令&下载后门

#章节点：
投递钓鱼篇，流量加密篇，其他篇（待定）
```

演示案例：

- Ewomail-邮件系统-搭建&使用
- Ewomail&Swaks-邮件伪造发信人
- Ewomail&Gophish-邮件加网页钓鱼
- 网页钓鱼-克隆修改-二维码用户劫持
- 网页钓鱼-克隆修改-Flash 升级后门上线

#不存在 SPF

可直接利用 Swaks 伪造任意发信人邮箱地址

#存在 SPF

1、采用其他主流邮件进行突破

上节课已演示：网易 163 邮箱

2、采用第三方邮件系统进行突破

上节课已演示演示：SendCloud

smtp2go（速度慢但免费发送量大）

SendCloud（速度快但免费发送量少）

https://www.smtp2go.com/

https://www.sendcloud.net/

3、采用自己搭建 Ewomail 配合 Swaks

-转发地址域名由你指定注册

-不受限于其他系统的限制和风控

http://doc.ewomail.com/docs/ewomail/jianjie

https://blog.csdn.net/u012866532/article/details/123335529

```
swaks --to 471656814@qq.com -f admin@a1iyun.com --data test.eml --server smtp.a1iyun.com -p 25 -au admin@a1iyun.com -ap xiaodi123
```

#优化平台-内容&钓鱼&批量-Gophish

https://github.com/gophish/gophish

1、使用已知邮箱系统

2、自建域名邮箱系统

#网页钓鱼-克隆修改

克隆：

1、手工另存为

2、Setoolkit

3、Goblin

https://github.com/xiecat/goblin

https://github.com/trustedsec/social-engineer-toolkit

修改：

1、网页代码-逻辑修改

2、EXE 后门-资源修改

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址