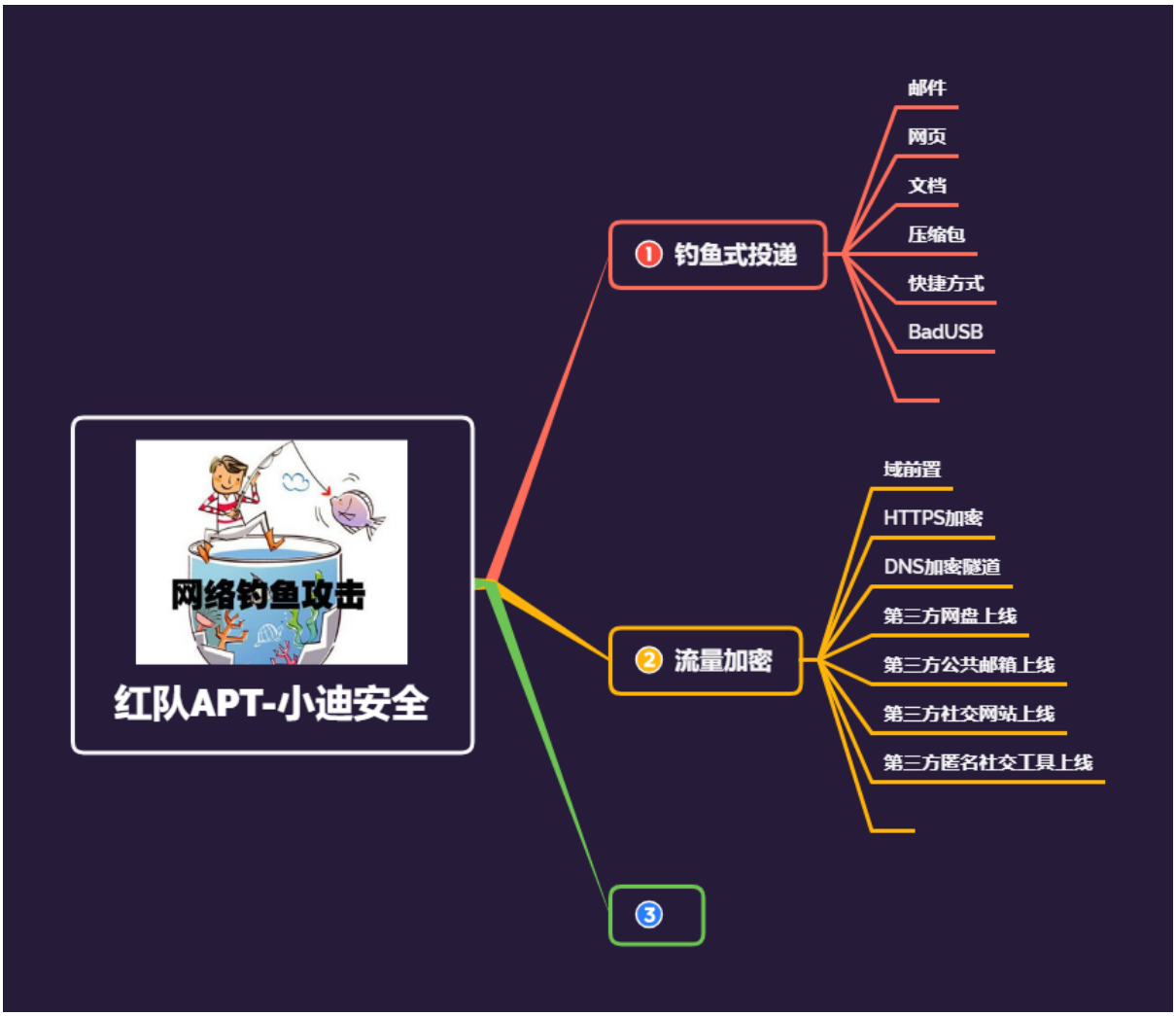
红队 APT-钓鱼篇&Office-CVE 漏洞&RLO 隐藏&压缩包释放&免杀打包捆绑



#知识点：

1、文件名-RLO 伪装-后缀

2、压缩文件-自解压-运行

3、捆绑文件-打包加载-运行

4、Office 套件-漏洞钓鱼-CVE

#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：

- 文件后缀-钓鱼伪装-RLO
- 压缩文件-自解压-释放执行
- 捆绑文件-打包加载-释放执行
- Office 套件-CVE 漏洞-MSF&CS
- 免杀方案-对象-EXE 文件&捆绑器

#文件后缀-钓鱼伪装-RLO

#压缩文件-自解压-释放执行

演示环境：Winrar 压缩软件

测评火绒

1.exe 游戏安装包

2.exe 后门（免杀火绒，但不免杀管家）

压缩运行 火绒不报毒

捆绑打包 火绒不报毒

测评管家

1.exe 游戏安装包

http.exe 后门（免杀管家，但不免杀火绒）

压缩运行 管家不杀（用 winrar）

第一个捆绑打包 管家查杀（用捆绑工具第三方）

第二个捆绑打包 管家不杀（用捆绑工具第三方）

#捆绑文件-打包加载-释放执行

1、过杀毒（白文件+免杀后门）

2、过释放（白文件+免杀后门+释放器）

#Office 套件-CVE 漏洞-MSF&CS

-Microsoft MSDT CVE-2022-30190 代码执行

https://github.com/JohnHammond/msdt-follina

该漏洞首次发现在 2022 年 5 月 27 日，由白俄罗斯的一个 IP 地址上传。恶意文档从 Word 远程模板功能从远程 Web 服务器检索 HTML 文件，

通过 ms-msdt MSProtocol URI 方法来执行恶意 PowerShell 代码。感染过程利用程序 msdt.exe，该程序用于运行各种疑难解答程序包。

此工具的恶意文档无需用户交互即可调用它。导致在宏被禁用的情况下，恶意文档依旧可以使用 ms-msdt URI 执行任意 PowerShell 代码。

目前已知影响的版本为：

office 2021 Lts

office 2019

office 2016

Office 2013

Office ProPlus

Office 365

测试：

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址