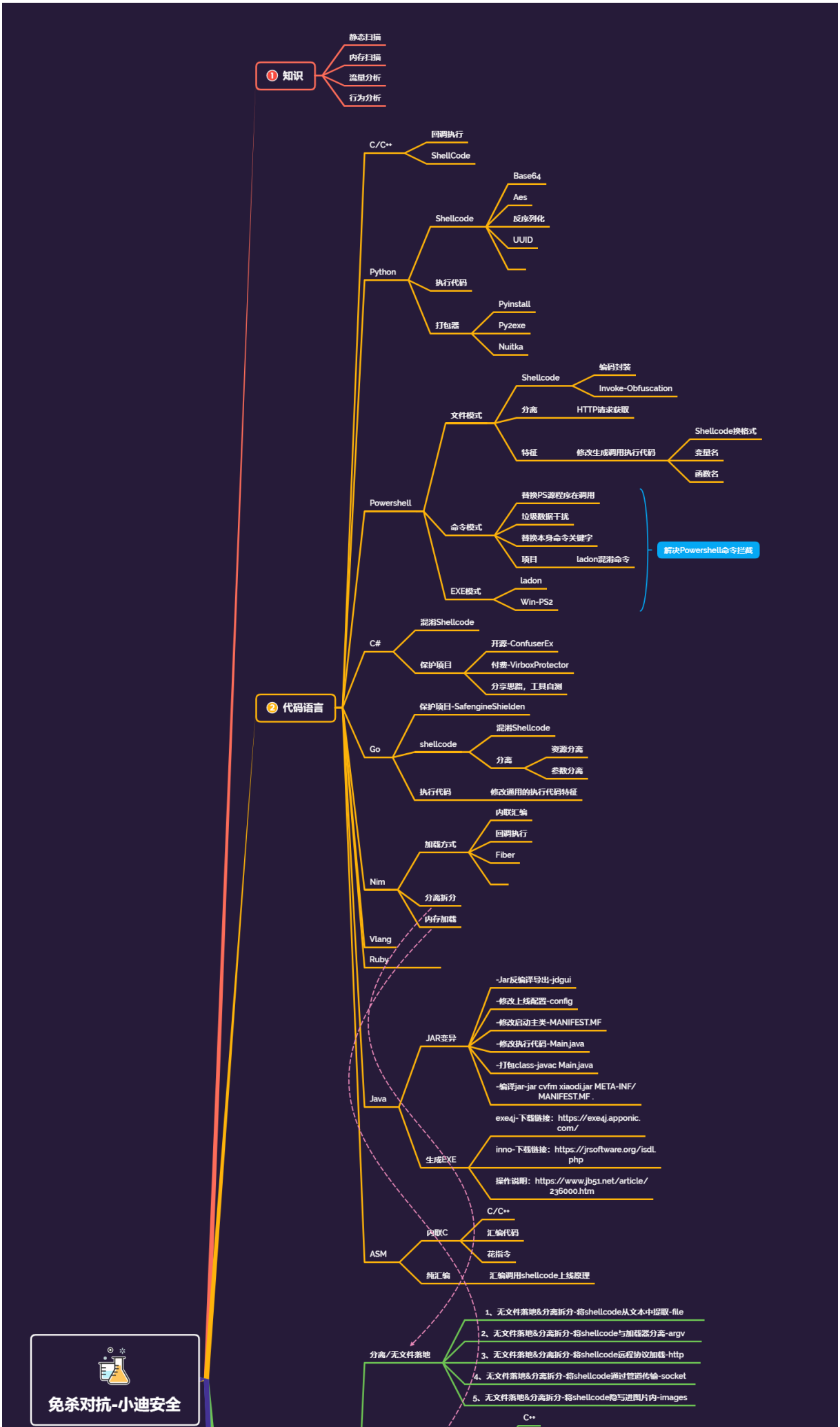
免杀对抗-Office 套件&VBA 宏&本地远程引用&混淆分离&保护密码


免杀对抗-小迪安全
① 知识
静态扫描
内存扫描
流量分析
行为分析
② 代码语言
C/C++
回调执行
ShellCode
Python
Shellcode
Base64
Aes
反序列化
UUID
执行代码
打包器
Pyinstall
Py2exe
Nuitka
Powershell
文件模式
Shellcode
编码封装
Invoke-Obfuscation
分离
HTTP请求获取
特征
修改生成调用执行代码
Shellcode换格式
变量名
函数名
命令模式
替换PS源程序在调用
垃圾数据干扰
替换本身命令关键字
项目
ladon混淆命令
解决Powershell命令拦截
EXE模式
ladon
Win-PS2
C#
混淆Shellcode
保护项目
开源-ConfuserEx
付费-VirboxProtector
分享思路，工具自测
Go
保护项目-SafengineShielden
shellcode
混淆Shellcode
分离
资源分离
参数分离
执行代码
修改通用的执行代码特征
Nim
加载方式
内联汇编
回调执行
Fiber
分离拆分
内存加载
Vlang
Ruby
Java
JAR变异
-Jar反编译导出-jdgui
-修改上线配置-config
-修改启动主类-MANIFEST.MF
-修改执行代码-Main.java
-打包class-javac Main.java
-编译jar-jar cvfm xiaodi.jar META-INF/MANIFEST.MF .
生成EXE
exe4j-下载链接：https://exe4j.apponic.com/
inno-下载链接：https://jrsoftware.org/isdl.php
操作说明：https://www.jb51.net/article/236000.htm
ASM
内联C
C/C++
汇编代码
花指令
纯汇编
汇编调用shellcode上线原理
分离/无文件落地
1、无文件落地&分离拆分-将shellcode从文本中提取-file
2、无文件落地&分离拆分-将shellcode与加载器分离-argv
3、无文件落地&分离拆分-将shellcode远程协议加载-http
4、无文件落地&分离拆分-将shellcode通过管道传输-socket
5、无文件落地&分离拆分-将shellcode隐写进图片内-images
C++

#知识点：

Office 套件-本地宏引用-保护密码

Office 套件-本地宏引用-工具项目

Office 套件-本地宏引用-混淆 VBA

Office 套件-远程宏引用-混淆 VBA

#章节点：

编译代码面-ShellCode-混淆

编译代码面-编辑执行器-编写

编译代码面-分离加载器-编写

程序文件面-特征码定位-修改

程序文件面-加壳花指令-资源

代码加载面-Dll 反射劫持-加载

权限逻辑面-杀毒进程干扰-结束

工具数据面-通讯内存流量-动态

对抗目标：

X60 Defender 某绒 管家 VT 等

编程语言：

C/C++ Python C# Go Powershell Ruby Java ASM NIM Vlang 等。

涉及技术：

ShellCode 混淆，无文件落地，分离拆分，白名单，DLL 加载，Syscall，加壳加花，资源修改，特征修改，二次开发 CS，内存休眠，进程注入，反沙盒，反调试，CDN 解析等

演示案例：

- Office 套件-本地宏引用-保护密码
- Office 套件-本地宏引用-工具项目
- Office 套件-本地宏引用-混淆 VBA

➢ Office 套件-远程宏引用-混淆 VBA

#Office 套件-本地宏引用-保护密码

保护密码&原型后缀&宏模版后缀

#Office 套件-本地宏引用-工具项目

https://github.com/outflanknl/EvilClippy

EvilClippy -s 1.vba xd.doc

```
Sub Hello()
Dim X
X=MsgBox("Hello VBS")
```

#Office 套件-本地宏引用-混淆 VBA

VBA 代码助手 macro_pack

BadAssMacrosx-i payload.bin -w doc -p no -s classic -c 5 -o 1.vba

https://github.com/lgzcarson/Payloads/blob/3066615cde55f9cd6755ed81a7d83c229f78e397/Methodology%20and%20Resources/Office%20-%20Attacks.md

#Office 套件-远程宏引用-混淆 VBA

1、制作包含宏的恶意模版文件（.dotm）。

2、将恶意模版文件上传至服务器。如 Github 等公共文件平台。

3、新建并保存一个使用任意模版的 docx 文件。

解压 docx 文件，修改 word_rels\settings.xml.rels 文件的 Target 属性，将其指向部署恶意模版文件的服务器。

4、使用 zip 格式压缩文件，并重新命名后缀为 docx。

5、重新打开 docx 文件，并启用宏。

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址