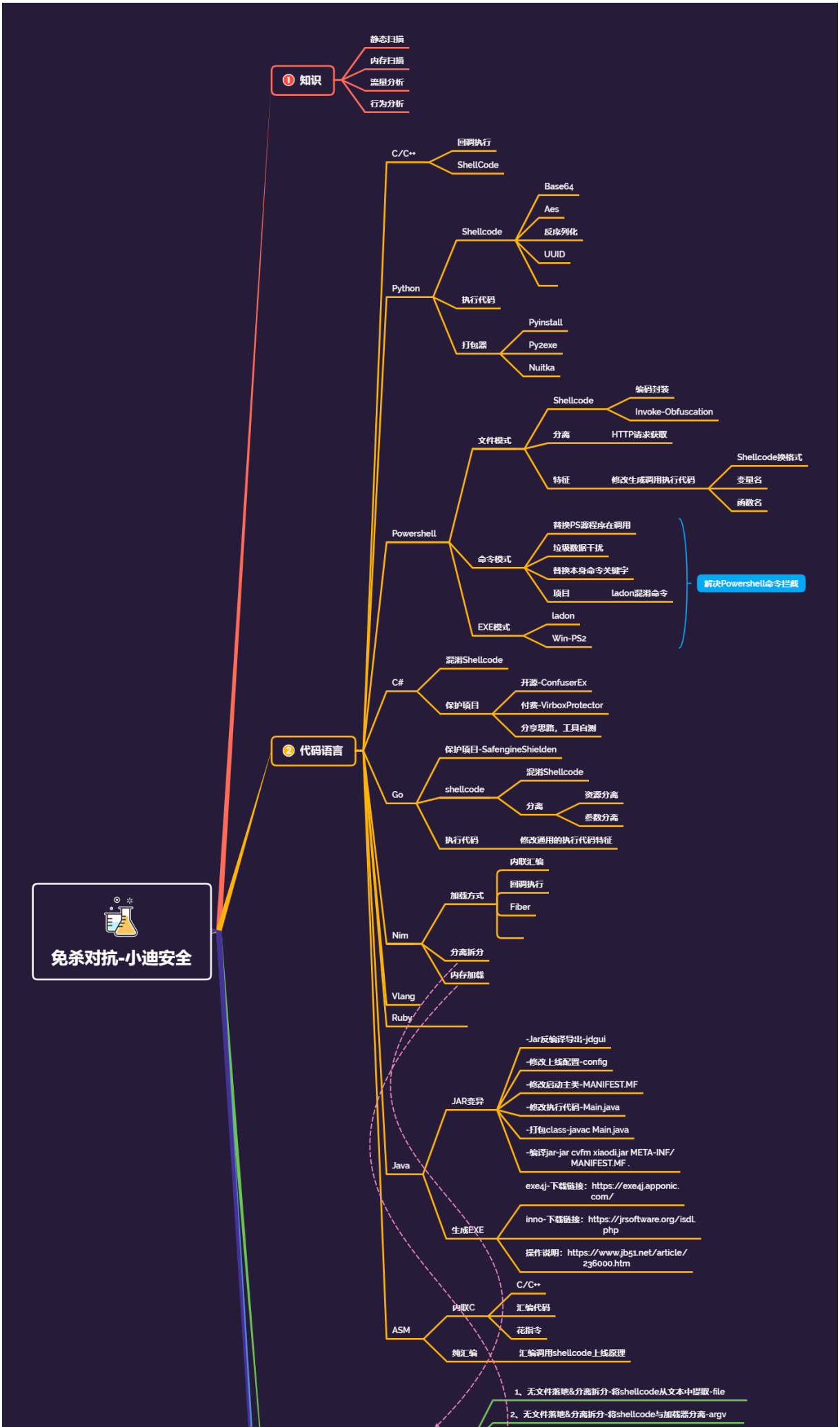
免杀对抗-特征码定位&添加花指令&加冷门壳&加反 VT 保护&资源修改


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
EXE模式
ladon
Win-PS2
解决Powershell命令拦截
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
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

#知识点：

1、特征码扫描-花指令&定位修改

2、文件检验法-资源修改&加签名

3、沙盒检测法-冷门壳&代码运行保护

#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：

- 成品 EXE-反特征码-通用跳转&花指令
- 成品 EXE-反 VT 沙盒-加壳加保护加资源

常见查杀方式理论点：

1、特征码扫描：所谓特征码其实就是程序内部的一串或者几串二进制机器码。特征码匹配工作原理是先总结出某个病毒的特征码，然后在目标文件中搜索看有没有类似的匹配，如果有匹配就暂定为病毒文件。优点：速度快，配备高性能的扫描引擎；准确率相对比较高，误杀操作相对较少；很少需要用户参与。缺点：采用病毒特征代码法的检测工具，面对不断出现的新病毒，必须不断更新病毒库的版本，否则检测工具便会老化，逐渐失去实用价值；病毒特征代码法对从未见过的新病毒，无法知道其特征代码，因而无法去检测新病毒；病毒特征码如果没有经过充分的检验，可能会出现误报，数据误删，系统破坏，给用户带来麻烦。

2、文件和校验法：将正常文件 A 的 hash 值保存，然后如果有一个新的 A 文件发送过来计算其 hash 值，如果与正常文件的不同，那么认定为病毒文件。

3、沙盒检测：基于行为的检测，看有没有一些敏感的行为来确定文件是否为病毒。优点是可能发现未知的病毒，缺点是误报相对较高，需要用户参与。

4、云查杀：类似于特征码查杀。只是如果特征码库没有匹配值的时候会把文件上传到云端继续分析，有时候扫描病毒刚扫描出来不是病毒，但过一会儿扫描就是病毒了，这种行为就是云查杀。

#成品 EXE-反特征码-通用跳转&花指令

1、C/C++-Project4-通用跳转法

特征码区域汇编移动到全 0 区域后用 jmp 调用

2、C/C++-Project2-花指令改入口

添加花指令重定向修改入口地址从而打乱特征码位置

#成品 EXE-反 VT 沙盒-加壳加保护加资源

加壳：Py-Pyinstall-UPX 等

加资源：Py-Pyinstall-Restorator

加保护：C-Project2-VMProject Shielden 等

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址