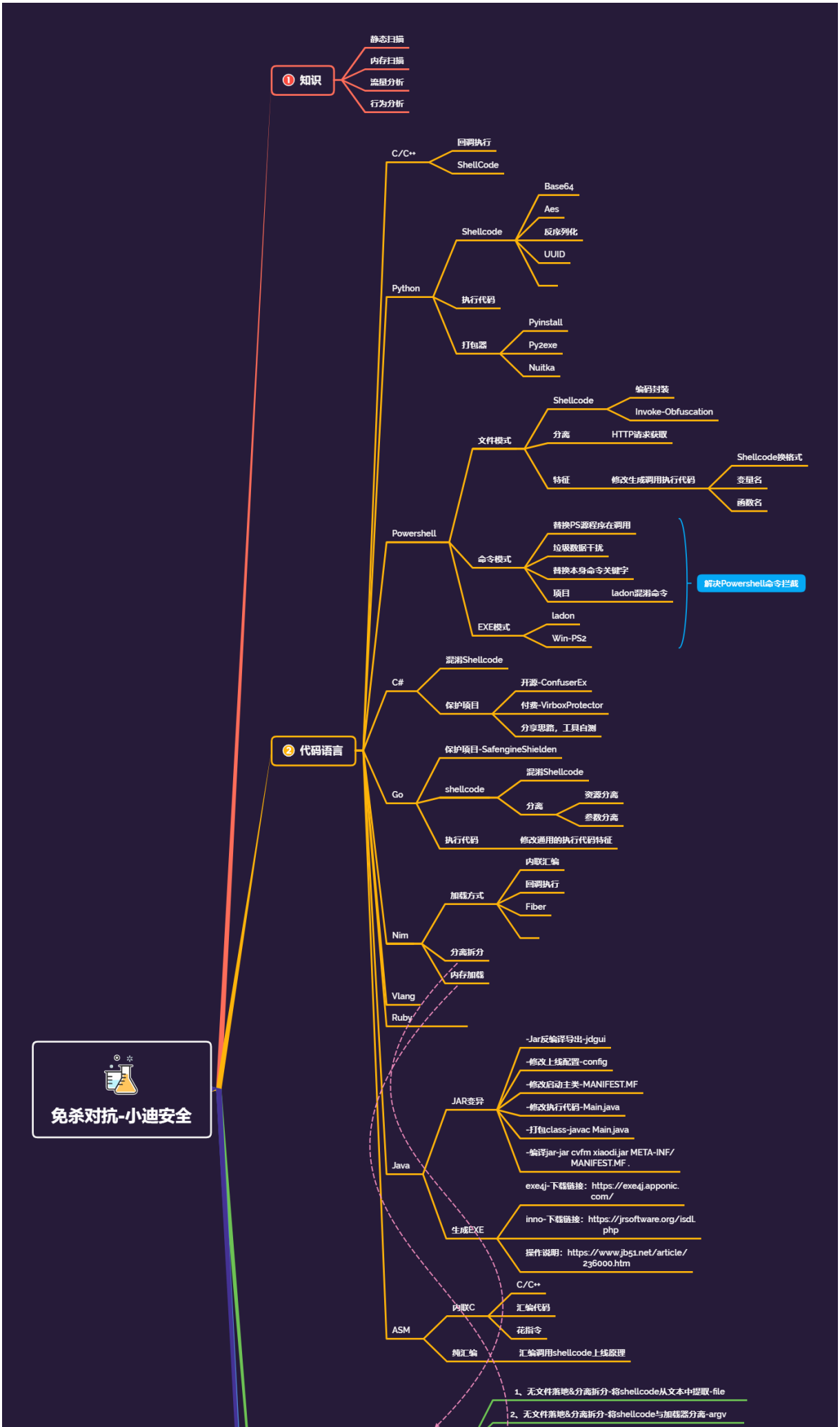
免杀对抗-反 VT 沙盒&反虚拟机&反调试&进程 APC 注入&项目保护


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
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、反 VT-沙盒检测-Go&Python&C++

2、反调试-调试检测&进程注入-C++

3、反 VT 反调试-程序保护-工具项目类

#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：

- 反 VT-沙盒检测-Go&Python&C++
- 反调试-调试检测&进程注入-C++
- 反 VT 反调试-程序保护-工具项目类

近年来，各类恶意软件层出不穷，反病毒软件也更新了各种检测方案以提高检测率。
其中比较有效的方案是动态沙箱检测技术，即通过在沙箱中运行程序并观察程序行为来判断程序是否为恶意程序。为了逃避沙箱/安全人员的检测，恶意软件使用了各类识别沙箱/虚拟机的技术，用于判断自身程序是否运行在沙箱/虚拟机中。

一、调试器检测

- 基本的例如 IsDebuggerPresent API ，PEB.BeingDebugged...
- TLS 回调
- hard/software breakpoints
- VirtualAlloc

...

二、DLL 注入检测

- 检测是否有 DLL 注入此进程来实现对进程的行为监控（HOOK）

三、Virtual Box 检测

- 检测文件，例如 VBoxMouse.sys， VirtualBox Guest Additions directory...
- 检测注册表，进程，服务，例如 VBoxControl.exe， VBoxService...
- 检测硬件名称，MAC 地址等等...

四、VMware 检测

- 与 VB 检测类似

五、其他虚拟平台检测

- 例如 Xen, QEMU, Wine, Paralles...

六、分析工具进程检测

- 检测例如 OD, ProcessMonitor, Autorun 等分析工具进程的存在....

七、通用沙盒/虚拟机检测

- 检测是否存在特殊进程名，模块名
- 通过 WMI 检测真实硬件状态，例如硬盘大小，内存大小，CPU 风扇，型号，BIOS 序列号名称，电源电压，温度等等...

1、微步沙盒：https://s.threatbook.cn/
2、腾讯哈勃分析系统：https://habo.qq.com/
3、魔盾：https://www.maldun.com/analysis/
4、微点沙盒：https://sandbox.depthsec.com.cn/index.php/

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址