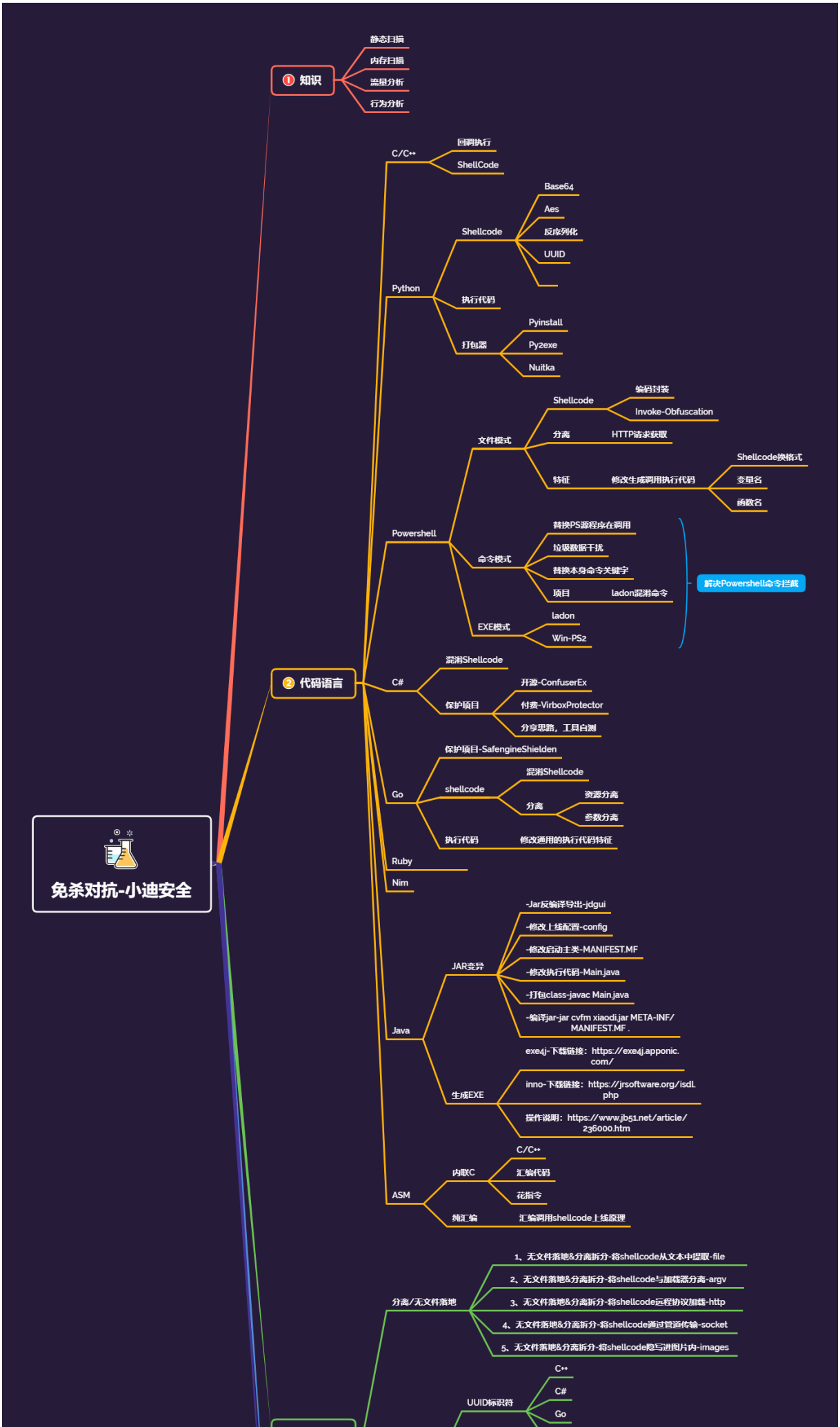
免杀对抗-Nim 语言&分离无文件 socket&隐写&参数化&内存加载 uuid 等


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
Ruby
Nim
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
UUID标识符
C++
C#
Go

#知识点：

1、Nim-加载工具-NimLoader

2、Nim-加载方式-OffensiveNim

2、Nim-分离加载-Socket&Http&Image

3、Nim-内存加载-UUID

#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：

- Nim-加载工具-NimLoader
- Nim-加载方式-OffensiveNim
- Nim-加载分离-Socket&Http&Image

➢ Nim-加载内存-UUID&OffensiveNim

一般的编译参数：

c：编译成 C 语言。例如：nim c test.nim

cpp：编译成 C++语言。例如：nim cpp test.nim

objc：编译成 objc 语言

js：编译成 javascript 脚本，可以建一个 html 文件在<script src="test.js"></script>里运行.

-d:release：进行 release 编译。nim cc -d:release test.nim

-r：编译完成后运行程序

--cincludes：包含 当前目录(./)的 c 头文件.

--cpu：指定架构，如：nim cc -cpu amd64 ， nim cc -cpu:arm。--cpu 参数有：i386, m68k, alpha, powerpc, powerpc64, powerpc64el, sparc, vm, hppa, ia64, amd64, mips, mipsel, arm, arm64, js, nimvm, avr, msp430, sparc64, mips64, mips64el, riscv64, esp, wasm32

编译 x64

```
nim c -d:mingw --app:gui --cpu:amd64 -d:danger -d:strip --opt:size --passc=-flto --passl=-flto test.nim
```

编译 x86

```
nim c -d:mingw --app:gui --cpu:i386 -d:danger -d:strip --opt:size --passc=-flto --passl=-flto test.nim
```

安装库：

```
nimble install
```

https://github.com/byt3bl33d3r/OffensiveNim

https://github.com/aeverj/NimShellCodeLoader

https://github.com/ScxMes/Core-Nim-programming

https://mp.weixin.qq.com/s/YKkCcqeiQLwyw4cJvQHilA

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址
