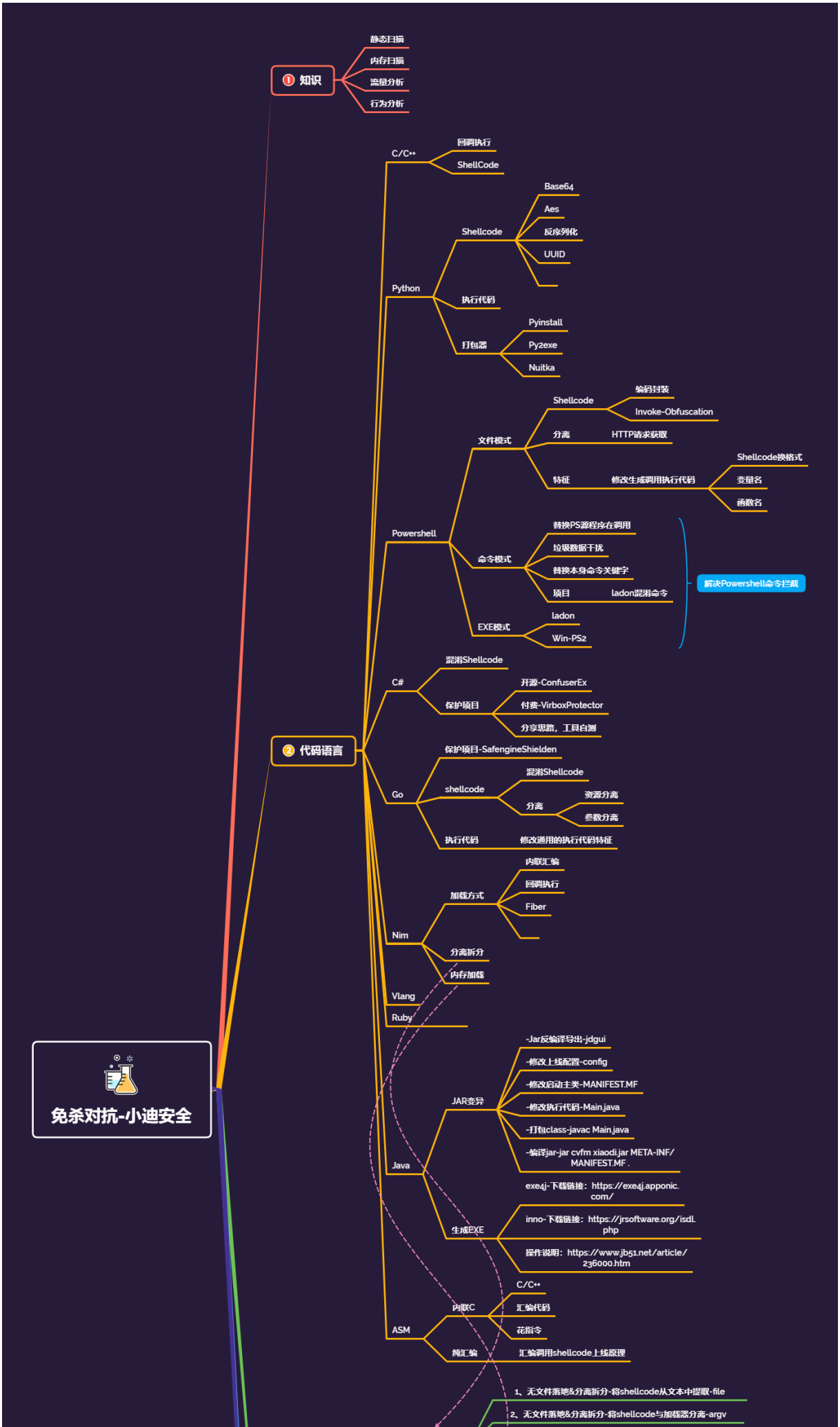
免杀对抗-二开 CS&上线流量特征&Shellcode 生成机制&反编译重打包(上)


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、CS-表面特征消除

2、CS-HTTP 流量特征消除

3、CS-Shellcode 特征消除

#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：

- 魔改搭建-CS 反编译及导入 IDEA 编译
- 表面配置-对端口密码证书做特征消除
- 逆向源码-对 http/s 上线流量做特征消除
- 逆向源码-对 http/s 生成 Payload 做特征消除

➢ 逆向源码-对 Powershell 生成 Payload 做特征消除

#反编译魔改 CS 项目搭建及修改过程：

环境：IDEA JDK8&11

参考：https://github.com/zer0yu/Awesome-CobaltStrike

1、反编译 Jar 包

2、新建 Java 项目

3、修改上线代码

4、打包替换编译

5、替换服务客户端

-反编译：

```
java -cp IDEA_HOME/plugins/java-decompiler/lib/java-
decompiler.jar
org.jetbrains.java.decompiler.main.decompiler.ConsoleDecompiler -
dgs=true <src.jar> <dest dir>
```

-具体命令：

```
"D:\program files\Java\jdk11\bin\java.exe" -cp "C:\Program
Files\JetBrains\IntelliJ IDEA 2022.1.3\plugins\java-
decompiler\lib\java-decompiler.jar"
org.jetbrains.java.decompiler.main.decompiler.ConsoleDecompiler -
dgs=true cobaltstrike.jar coba
```

#表面配置-对端口密码证书做特征消除

简单说下，较为简单，主要是源码的特征流量

•cobaltstrike.beacon_keys 和 cobaltstrike.store 不要使用默认的文件，删除

•profile 文件要换新的，启动服务端时记得加载，或直接把 jar 包里面的默认配置给改了

•开在公网的 teamserver 不要使用默认端口

https://github.com/zer0yu/Awesome-CobaltStrike

#逆向源码-对 http/s 上线流量做特征消除

checksum8 函数对比后续-common\CommonUtils&cloudstrike\WebServer

80：http://IP/aaa9

443：https://ip:443/aaa9

当然特征不止这一个「aaa9」例如「http://IP/HjIa」这个也会出现这种状态

只要是符合「checksum8」算法技术出来的文件都可以请求到 「不是唯一值」

```
public class EchoTest {
    public static long checksum8(String text) {
        if (text.length() < 4) {
            return 0L;
        }
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址