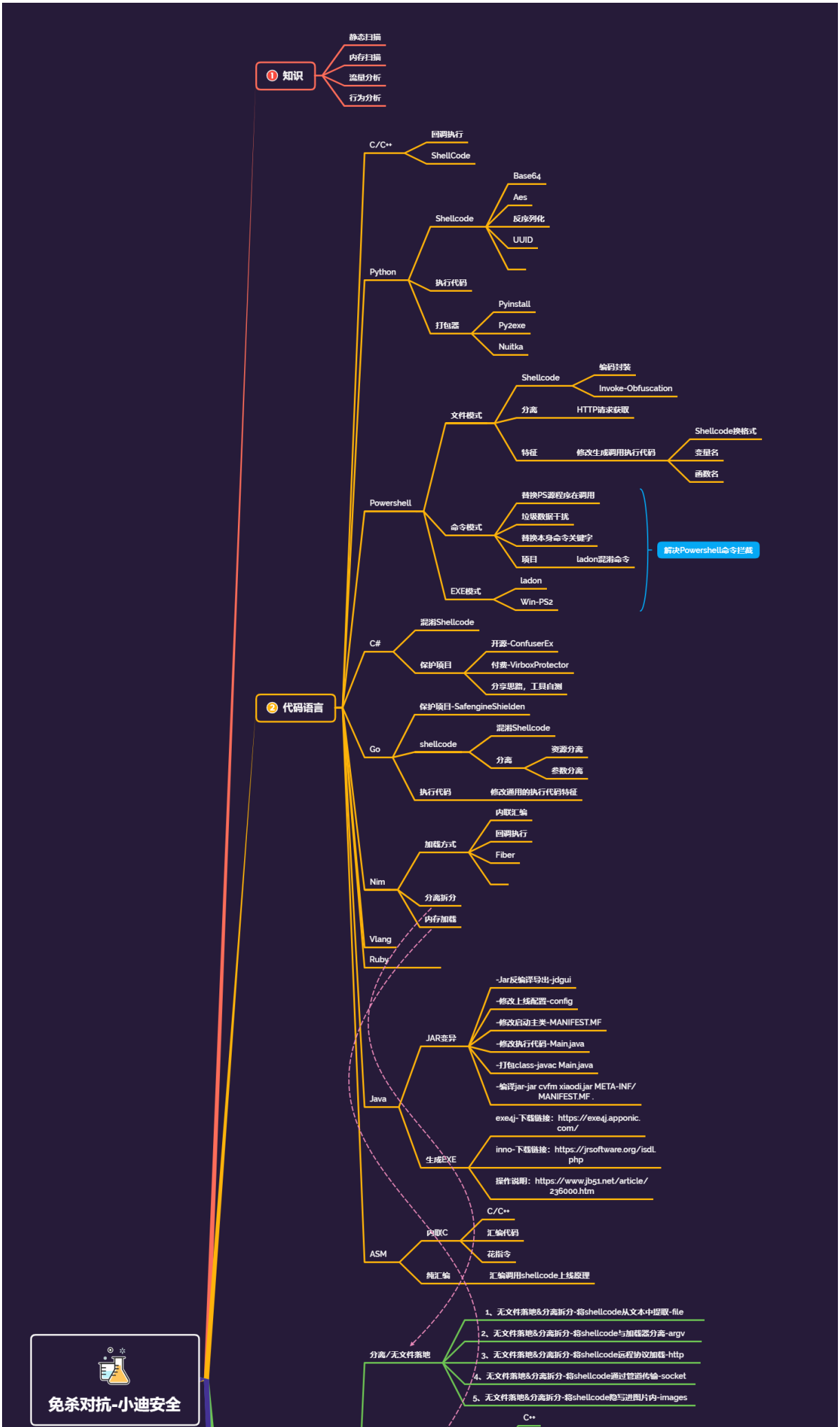
免杀对抗-防朔源&防流量&防特征&CDN 节点&SSL 证书&OSS 存储&上线


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-CDN 节点-防拉黑

2、CS-SSL 证书-防特征

3、CS-OSS 存储-防流量

#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：

- 防朔源拉黑-CDN 节点-上线
- 防特征审计-SSL 证书-上线
- 防流量审计-OSS 存储-上线

#防朔源拉黑-CDN 节点-上线

https://sg.godaddy.com/

https://dash.cloudflare.com/

https://github.com/threatexpress/malleable-c2

1、注册账号，申请狗爹域名

2、注册账号，配置 cloudflare

3、添加解析记录，指向 CS 的 IP

4、配置 DNS 服务器，使用 cloudflare

5、下载 C2 文件模版，修改配置并上传

6、启动 CS 加载 CS 模版，使用 stag 生成

注意 1：

因为 cloudflare 的原因这里端口的设置需要注意以下：

若是 http，则只能设置 80,8080,8880,2052,2082,2086,2095 这些端口号

若是 https，则只能设置 443,2053,2083,2087,2096,8443 这些端口号

注意 2：

后门生成使用 Stageless 模式

#防特征审计-SSL 证书-上线

1、配置 SSL 设置

-创建证书（SSL-源服务器）

-设置页面规则(缓存级别-绕过)

-保存 CSR&密匙(server.pem&server.key)

2、生成证书文件

```
openssl pkcs12 -export -in server.pem -inkey server.key -out
www.yaosese.xyz.p12 -name www.yaosese.xyz -passout pass:123456
keytool -importkeystore -deststorepass 123456 -destkeypass 123456
-destkeystore www.yaosese.xyz.store -srckeystore
www.yaosese.xyz.p12 -srcstoretype PKCS12 -srcstorepass 123456 -
alias www.yaosese.xyz
```

3、修改 teamserver

证书指向：www.yaosese.xyz.store

证书密码：123456

4、启动 teamserver

```
./teamserver ip pass jquery-c2.4.5.profile
```

#防流量审计-OSS 存储-上线

产品：阿里云，腾讯云等

1、开启 OSS 对象存储

2、创建 Bucket 列表

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址