<黑客免杀攻防>第五章 花指令与免杀 读书笔记

原创

dalerkd 于 2014-11-04 21:27:50 发布 874 收藏
分类专栏： 苦行僧之路 读书笔记

本文链接：https://blog.csdn.net/dalerkd/article/details/40793729


苦行僧之路 同时被 2 个专栏收录
57 篇文章 0 订阅
订阅专栏


读书笔记
28 篇文章 1 订阅
订阅专栏

1为了保护真正的果实,所以使用花朵是别人迷惑.

花指令不是加密代码,它分两种:

a夹杂运行

b高级语言的花指令应用,程序在运行时会因为花指令而改变原有的流程.该书暂不涉及,据称"比较复杂且效果有限"

2脚本木马花指令

3花指令根基-汇编语言

a认识汇编

80x86汇编大致可分为这么几个功能组:

- 数据传输指令
- 逻辑运算指令
- 串操作指令
- 控制转移指令
- 处理器控制指令

b增加反汇编添加任意功能:

知识点:汇编调用API函数遵循sdtcall调用规则(从右到左的压栈)

对于少数API使用的是cdecel例如printf

理论上设计一个简单粗暴的恶意程序:再删除C盘下所有能删除的东西.先尝试格式化其它盘并用垃圾数据覆盖.

更加说明了安全软件接管暴力命令的必要性以及访问权限的控制.

4花指令入门

A常用花指令

- nop
- pop 0;pop 0
- push ebp;pop ebp
- add esp,1;sub esp,1
- add esp,1;add esp,-1
- sub esp,1;sub esp,-1
- inc exc;dec exc
- sub eax,-2;dec eax;dec eax
- push ******;retn ///将入口地址压入栈,再返回到入口地址
- mov eax,*****;jmp eax

两种反汇编算法:

1. 递归行进
2. 线性扫描

"Softice和Windbg属于前者，OD和IDA属于后者。
对于线性扫描，我们在代码段加入数据定义来迷惑反编译器，比如在汇编代码中嵌入：
_asm _emit 0x0f;//_EMIT伪指令相当于MASM中的DB，但一次只能定义一个字节。
这样会让部分反编译器错误的将其错误识别。
递归遍历比较高级，简单的插入定义起不到作用。可以将_asm _emit 0x0f放在永远不能达到的条件分支后，比如比较1和1不相等则转跳。这样可以迷惑IDA，对OD无效。可能它对不同的分支都做了分析。
解决方式是：在转跳的目的的起始位置定义。"---摘自看雪论坛<反调试跟踪的一点心得>作者"质量第一"

使用emit伪指令直接插入机器码在内嵌汇编中,可能(当这种花指令符合OPCode规则时)导致OD错误翻译下文.

5花指令在免杀领域的应用

A

B修改技巧

不在不可控的情况下破坏堆栈平衡

C寻找空白区域,加空白区段

1用WinHex寻找

2检查区域是否可写

PEID也可以完成这个任务哟,CodeCaver(PE空隙搜索器)是专门寻找0x00区域的程序(**注意:**它只能在目标文件运行的情况下寻找,如果是木马汗)

可以用ToPo来增加空白区段.

6花指令的高级应用-提取,快速应用,SEH

A花指令的提取与快速应用

B SEH异常的应用

SEH异常又名结构化异常处理,是系统提供的一个服务,用于使软件更健壮.

"Win32结构化异常处理是操作系统提供的一种服务。 在编译器的 SEH 层减少了直接使用纯操作系统的 SEH所带来的危害的同时，也将纯

操作系统的 SEH 从大家的面前隐藏了起来。

但程序遇到Seh异常时，异常交给系统处理（这将是一个非常负责的过程，很容易跟飞），所以利用Seh异常可以一定程度的防止程序被调试。（seh异常在壳里是很常见的）"

--摘自 ZanipoLo的新浪博客 其内有详细介绍和使用方法.