Rootkit的学习与研究【转自看雪】

转载

clearver 于 2010-01-18 21:03:00 发布 883 收藏
分类专栏： 病毒木马 文章标签： hook windows dll object command 网络

Rootkit是什么？估计很多朋友并不明白，简单的说，Rootkit是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，比较多见到的是Rootkit一般都和木马、后门等其他恶意程序结合使用。Rootkit通过加载特殊的驱动，修改系统内核，进而达到隐藏信息的目的。技术是双刃剑，我们研究它的目的在于，透过我们的研究，用这项技术来保护我们的系统，使我们的系统更加健壮，充分发挥这个技术的正面应用。

对于ROOTKIT专题的研究，主要涉及的技术有如下部分：

1. 内核hook

对于hook，从ring3有很多，ring3到ring0也有很多，根据api调用环节递进的顺序，在每一个环节都有hook的机会，可以有int 2e或者sysenter hook，ssdt hook，inline hook ，irp hook，object hook，idt hook等等。在这里，我们逐个介绍。

1）object hook
2）ssdt hook
3）inline-hook
4）idt hook
5）IRP hook
6）SYSENTER hook
7）IAT HOOK
8）EAT HOOK

2. 保护模式篇章第一部分： ring3进ring0之门

1)通过调用门访问内核
2)通过中断门访问内核
3)通过任务门访问内核
4)通过陷阱门访问内核

3。保护模式篇章第二部分：windows分页机制

1）windows分页机制

4。保护模式篇章第三部分：直接访问硬件

1）修改iopl，ring3直接访问硬件
2）追加tss默认I/O许可位图区域
3）更改tss I/O许可位图指向

5。detour 修改函数执行路径，可用于对函数的控制流程进行重定路径。

1）detour补丁

6. 隐身术
1）文件隐藏
2）进程隐藏
3）注册表键值隐藏
4）驱动隐藏
5）进程中dll模块隐藏
6）更绝的隐藏进程中的dll模块，绕过IceSword的检测
7）端口隐藏

7。ring0中调用ring3程序
1) apc方式
2) deviceiocontrol 方式

8。进程线程监控
1）监控进程创建
2）杀线程
3）保护进程和屏蔽文件执行

9。其他
1）获取ntoskrnl.exe模块地址的几种办法
2）驱动感染技术扫盲
3）shadow ssdt学习笔记
4）高手进阶windows内核定时器之一
5）高手进阶windows内核定时器之二
6）运行期修改可执行文件的路径和Command Line
7）查找隐藏驱动
8）装载驱动的几种办法
9）内核中注入dll的一种流氓方法
10）另一种读写进程内存空间的方法
11）完整驱动感染代码
12）Hook Shadow SSDT
13）ring0检测隐藏进程

对于rootkit的研究，涉及到的内容比较多，需要在充分学习理解这些技术的前提下，透过目前网络上出现的一些rootkit病毒，木马来进行分析，做到活学活用。因此，对于本版块的思路很清晰，首先是基础技术理论的研究，由于目前windows还是主流的操作系统，因此，我们主要研究windows下的rootkit，这个课题是一个长期的，对这个课题感兴趣的朋友，欢迎大家一起参与讨论。