<<网络安全与管理技术实验教程>>

图书基本信息

书名：<<网络安全与管理技术实验教程>>

13位ISBN编号：9787308106375

10位ISBN编号：7308106373

出版时间：2012-12

出版时间：浙江大学出版社

<<网络安全与管理技术实验教程>>

书籍目录

章节摘录

版权页： 插图： 4.实验原理 （1）三线程软件工作原理。
大多数病毒只有一个进程或线程，当该进程或线程被杀死后病毒即告失效，因此易于查杀、存活率不高。
三线程类软件则因为其独特结构使得该类恶意软件无法被传统的内存杀毒软件成功查杀。
顾名思义，三线程软件由三个线程构成：一个病毒主体、两个监视器，三者之间相互监护、相互重生。
其中一个监视器（主体监视器）被注入到其他正常进程中，并在远程启动后时刻监视并保护病毒主体的运行：如果病毒主体被杀死，主体监视器即刻重生病毒主体并恢复其运行。
为了防止用户通过重启计算机的方式清除运行的恶意软件，软件在注册表中建立了其主程序的自启动项，同时通过另一个监视器（注册表监视器）监护该自启动注册表项：如果该表项被删除，注册表监视器即刻在注册表中重生该表项，保证无法通过重启方式影响病毒运行。
病毒主体除负责软件主体功能之外，还要监护主体监视器和注册表监视器，确保其中任何一个被杀死后即可重建并运行。
这种环环相扣的互保结构如图7—1所示。
T—Mouse恶意鼠标软件即为一种具备上述特征的三线程程序，其病毒主体的主要功能是影响鼠标定位和点击，使用户无法正常使用鼠标功能。
（2）COM文件结构。
COM文件具有一种结构最简单的单段可执行文件结构，其总大小（代码+数据）严格限制在64KB以内，执行时被完整地装入一个内存块中（称为段），因此各段寄存器内容均相同。
由于操作系统需要为装入的COM文件建立256字节的程序段前缀PSP和256字节的起始堆栈，因此COM文件的实际长度不能超过64×1024—512=65024字节，否则加载失败无法执行。
程序段前缀PSP的大小为100H，COM文件代码直接被装入PSP之后的空间，因此COM文件的第一条指令地址为100H。
COM文件结构如图7—2所示。
（3）恶意代码的寄生方式 按照恶意代码在宿主程序中的位置，常见寄生方式可分为三种：头寄生、尾寄生和插入寄生。
头寄生是指恶意代码寄生在宿主程序的前端，原位置的部分代码被转移至程序尾部，并通过在恶意代码段尾部安排跳转指令，在执行完恶意代码段后转到正常代码段执行。
尾寄生是指恶意代码寄生在宿主程序的末端，通过修改100H地址的第一条指令跳转到尾部首先执行恶意代码部分，随后再恢复100H地址的原指令执行正常程序代码。
插入寄生是指恶意代码寄生在宿主程序中间位置，同样通过跳转指令实现恶意代码和正常代码的接续执行。

<<网络安全与管理技术实验教程>>

编辑推荐

《高等院校计算机技术"十二五"规划教材:网络安全与管理技术实验教程》内容取材于“ 网络安全与管理技术 ”课程实验，从实验原理入手，由浅入深，逐步细化，对实验过程进行了细致翔实的描述，并针对实验过程提出了若干思考问题，既使学生掌握了基本的实验原理和实验步骤，也为学生进一步巩固和提高预留了空间，旨在使学生能更好地理解和掌握理论知识，并将其应用到实践中去，通过理论与实际的结合，切实提高实践能力。

<<网络安全与管理技术实验教程>>

版权说明