Vista系统下的恶意软件Rootkit攻防手册 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/276/2021_2022_Vista_E7_B3_BB_E7_BB_c67_276576.htm 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，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。 Windows vista自身对恶意软件的防护主要是通过驱动程序数字签名、用户访问控制(UAC)和WindowsDefender来实现的，前两者对Rootkit类恶意软件的防御尤为重要。因为Rootkit的隐藏功能实现需要加载驱动，我们就先说说Vista的驱动程序加载管理：Vista驱动程序的安装加载管理和原有的Windows版本相比有较大的改进，在Microsoft的设计中，Vista不允许加载没有经过数字签名的驱动程序，而在之前的Windows2000、XP、2003系统上，系统虽然会在安装未签名或老版本驱动程序时会有提示，但安装好之后是能够加载的。 出于Microsoft意料之外的是，“有数字签名的驱动程序才能被Vista所加载”这个设定对Rootkit类的防护作用并不是很大。去年的Blackhat会议上，曾有研究人员演示过在VistaX64Beta2版本上通过修改磁盘上页面文件来加载未经数字签名的驱动程序，虽然这个漏洞稍后被Microsoft补上，但已经说明通过技术手段来突破Vista的驱动加载管理并非不可能。但要突破Vista驱动加载管理的更好途径是在数字签名本身上做功夫，之前曾有安全研究人员提到，Vista驱动程序的数字签名申请的审核并不严格，只需要有合法的申请实体，并交纳少许的申请费用即可。 这样，通

过注册或借用一个公司的名义，Rootkit作者完全可以从Microsoft拿到合法的驱动数字签名，也就是说，很有可能会出现拥有Microsoft数字签名的、“ 合法 ”的Rootkit程序。攻击者还可以使用特殊的加载程序来加载没经数字签名的程序，安全公司LinchpinLabs最近就发布了一个叫做Astiv的小工具，这个工具实现的原理就是使用经过数字签名的系统组件来加载未经数字签名的驱动程序，而且用这种方式加载的驱动程序并不会出现在正常驱动程序列表中，更增强了加载目标驱动程序的隐蔽。 用户访问控制(UAC)是Vista防御恶意软件的另外一个手段 在开启了UAC的Vista系统上，用户的权限相当于被限制了的管理员权限，如果用户程序要对系统盘及注册表等地方进行修改的话，需要用户进行交互的二次确认。如果用户拒绝或者是目标程序比较特殊(比如木马、后门等)不出现UAC提示，因为对系统目录和注册表的访问被Vista所拒绝，除了极个别不写入系统目录的之外，大部分目标程序是无法安装成功的。Rootkit程序在UAC环境中同样会因为权限问题而无法安装成功，但很多情况下，攻击者会使用社会工程学的方法来诱骗用户信任攻击者所提供的程序，并在UAC提示时选择允许操作。 至此可以得出一个结论，由于WindowsVista从设计开始就很重视安全性，因此对它推出之前的Rootkit等恶意软件的防御水平到达了一个新的高度，攻击者单纯靠技术手段攻击的成功率已经比在原先的Windows2000/XP/2003平台上大为下降。但我们也应该注意到，攻击者会更多的使用社会工程手段，伪造和利用各种信任关系，欺骗用户安装恶意软件。 如何在Vista下对Rootkit类恶意程序进行防护?用户可以参考以下几点： 1、保持Vista的

系统补丁版本为最新。 2、不在不可信的来源获取软件，并在安装使用时留意系统的各种提示，尤其是有关数字签名的提示。 3、注意UAC的提示信息，及时拦截试图修改系统的危险操作。 4、使用反病毒软件并保持病毒库版本为最新，为防护恶意软件多加一层保障。 5、定期使用支持Vista的反Rootkit工具对系统进行扫描检查。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com