警惕底层Rootkit病毒新变种 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/460/2021_2022__E8_AD_A6_E6_83_95_E5_BA_95_E5_c100_460803.htm "系统侵蚀者"（Win32.Troj.AntiAV.e.172098）这是一个极具破坏性的病毒。当病毒一运行后，桌面立即会消失，而且无法对系统做任何的操作，能看见的只是一个蓝色的桌面而已。 "Rootkit25920"（Win32.TrojDownloader.HmirT.a.25920）这是一个Rootkit病毒。该病毒会监视userinit.exe和explorer.exe进程，创建、修改注册表启动项、服务项键，躲避安全监视工具，创建文件。一、"系统侵蚀者"（Win32.Troj.AntiAV.e.172098） 威胁级别：★★ 该病毒破坏能力立杆见影，除了立即使桌面消失以外，当用户重启机器后，会发现同样只显示蓝色的桌面，此时寻找支控桌面的explorer.exe系统文件时，会发现该系统文件已经被病毒删除。当我们使用ctrl alt del热键显示出任务管理器时，通过浏览方式查看到"我的电脑"图标已经被删除，变成默认的图标。该病毒会给用户的心理和系统已经造成严重的影响。 二、"Rootkit25920"（Win32.TrojDownloader.HmirT.a.25920） 威胁级别：★ 该病毒是一个rootkit深层病毒。该病毒会通过调用一些函数，通过函数避免安全软件的监视和截获。并且还会在注册中建立新的病毒键值，其服务名为saiujrh38l.其对应的病毒文件路径为：%System32%\DRIVERS\saiujrh38l.sys.该病毒会监视userinit.exe和explorer.exe系统进程，当监测到有userinit.exe启动时，则会恶意修改注册表的runonce项，通过用户在下次启动系统时触发病毒，其病毒对应的路径为

：%systemroot%\system32\55Id.dll.当病毒监测到有explorer.exe系统进程时，则创建一个新进程，其进程名为saiujrh38l.sys，对应路径是：%SystemRoot%\system32\drivers. 金山反病毒工程师建议 1.最好安装专业的杀毒软件进行全面监控。建议用户安装反病毒软件防止日益增多的病毒，用户在安装反病毒软件之后，应该经常进行升级、将一些主要监控经常打开（如邮件监控、内存监控等），遇到问题要上报，这样才能真正保障计算机的安全。 2.玩网络游戏、利用QQ聊天的用户会有所增多，所以各类盗号木马必将随之增多，建议用户一定要养成良好的网络使用习惯，及时升级杀毒软件，开启防火墙以及实时监控等功能，切断病毒传播的途径，不给病毒以可乘之机。 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