

NetSky蠕虫病毒样本分析报告 PDF转换可能丢失图片或格式
，建议阅读原文

https://www.100test.com/kao_ti2020/490/2021_2022_NetSky_E8_A0_95_E8_c67_490686.htm 病毒名称：Worm.Win32.NetSky.c
病毒类型：蠕虫类 文件 MD5：

FAC9D5A7A971CC4399F3AC9AAC1809F9 文件长度：7,168
字节 感染系统：Windows98以上版本 开发工具：Microsoft
Visual C 6.0 加壳类型：UPX 0.89.6 - 1.02 / 1.05 - 1.22 病毒描述

：该病毒为蠕虫类，病毒运行后复制自身到系统目录，并删除自身。创建服务，并以服务的方式达到随机启动的目的。

修改注册表，改变Internet Settings中的默认路径，由当前用户文件夹改为LocalService文件夹。该病毒可以盗取用户敏感信息。

行为分析：本地行为：1、文件运行后会衍生以下文件
%System32%\（病毒名）7,168 字节 2、创建服务，并以服务的方式达到随机启动的目的：服务名称：pangu_service_name

显示名称：盘古2007最新版本服务端 描述语言：盘古2007最新版本服务端 文件路径：%System32%\（病毒名）启动方式

：自动 3、修改注册表，改变Internet Settings中的默认路径，由当前用户文件夹改为LocalService文件夹。4、该病毒可以盗取用户敏感信息。

注释：%Windir% WINDODWS所在目录
%DriveLetter% 逻辑驱动器根目录 %ProgramFiles% 系统程序默认安装目录 %HomeDrive% 当前启动系统所在分区

%Documents and Settings% 当前用户文档根目录 %Temp% 当前用户TEMP缓存变量；路径为：%Documents and Settings%\当前用户\Local Settings\Temp %System32% 是一个可变路径；病毒通过查询操作系统来决定当前System32文件夹的位置；

Windows2000/NT中默认的安装路径是 C : \Winnt\System32 ;
Windows95/98/Me中默认的安装路径是 C : \Windows\System
; WindowsXP中默认的安装路径是 C : \Windows\System32. 清
除方案：1、使用安天木马防线可彻底清除此病毒（推荐）
，请到安天网站下载：www.antiy.com . 2、手工清除请按照行
为分析删除对应文件，恢复相关系统设置。推荐使用ATool（
安天安全管理工具），ATool下载地址：www.antiy.com
或<http://www.antiy.com/download/index.htm> . （1）使用安天木
马防线或ATool中的“进程管理”关闭病毒进程（2）强行删
除病毒文件 %System32%\（病毒名）（3）禁用服
务pangu_service_name 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