快捷方式类病毒的处理

——瑞星信息安全沙龙

主讲人：康传鹏

2011年11月04日

概述

1、两类快捷方式类病毒的处理过程

深入分析淘宝快捷方式和1KB快捷方式病毒，根据病毒行为，提供相应处理和防范措施；

2、瑞星网络版可以帮我们做什么

根据网络安全面临的问题，来分析瑞星能为我们的网络安全贡献什么；

3、易忽略的瑞星网络版实用功能

根据用户的反馈，总结几点大家容易忽略的网络版实用功能；

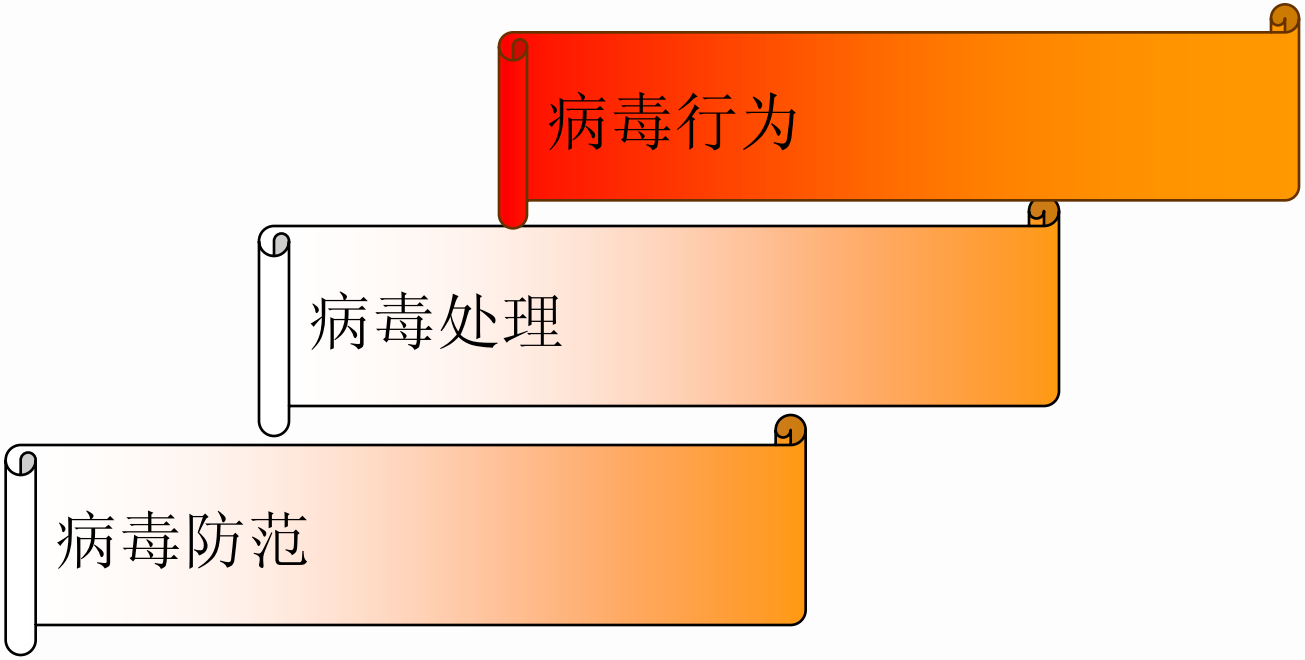
两类快捷方式类病毒的处理过程

两类快捷方式类病毒的处理过程

1、淘宝桌面快捷方式无法删除

2、1KB快捷方式（暴风一号）的处理过程

淘宝桌面快捷方式无法删除

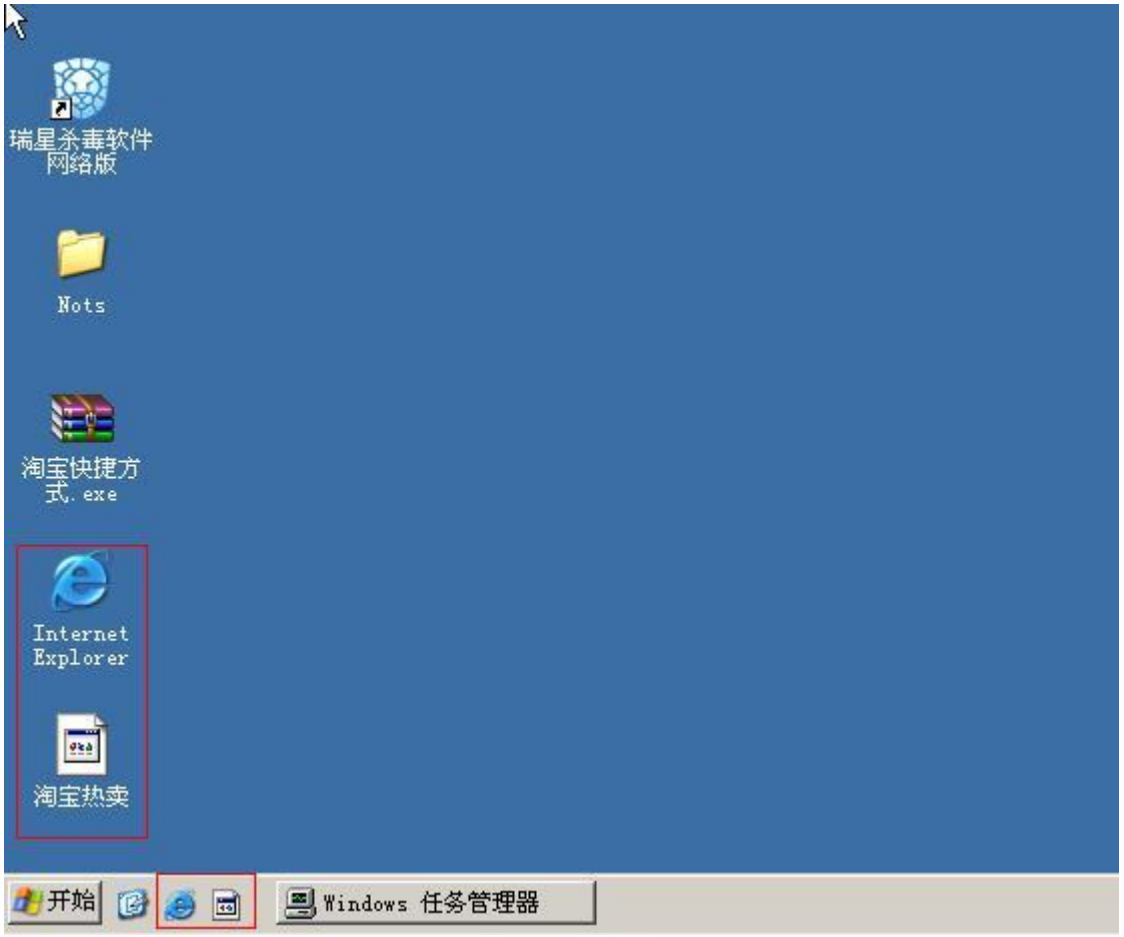


淘宝桌面快捷方式无法删除

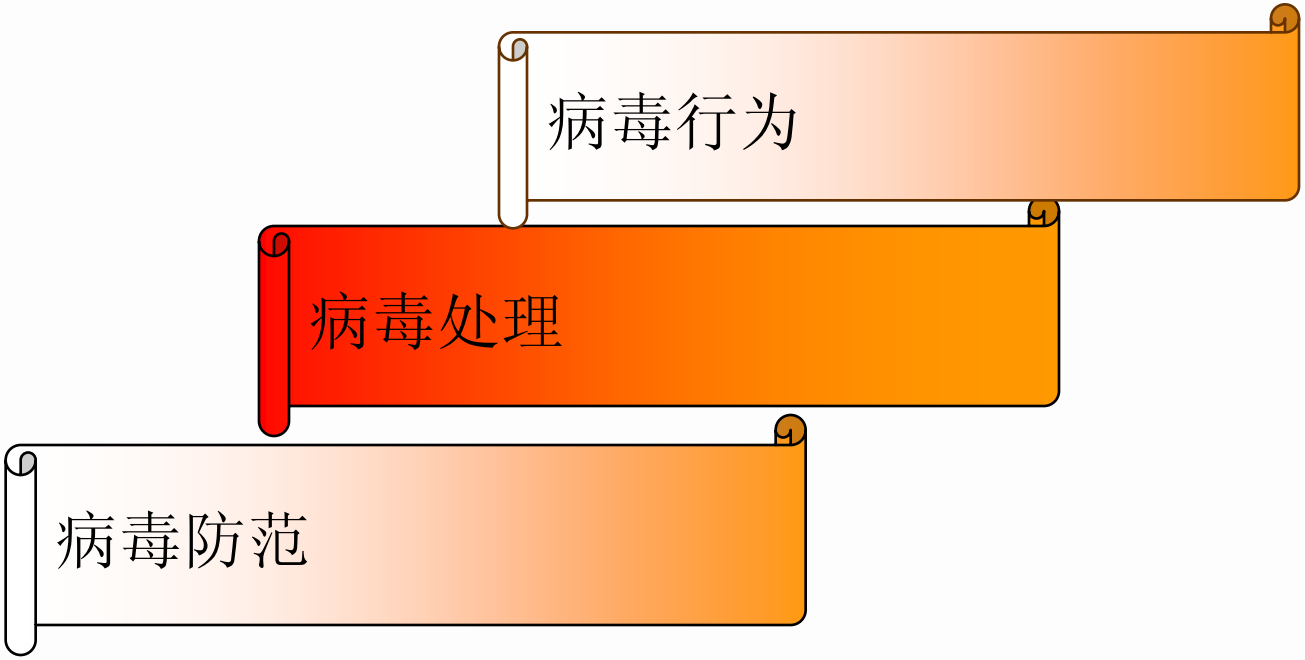
系统变慢，桌面多出个IE图标和淘宝热卖快捷方式，这类快捷方式手工无法删除，还会弹出恶意网站的网页。

多出的IE图标和淘宝热卖其实是 .iee、 .itt的快捷方式，双击这些快捷方式会调用C:\Program Files\Internet Explorer\iexplore.exe，打开特定的网站。

淘宝桌面快捷方式无法删除



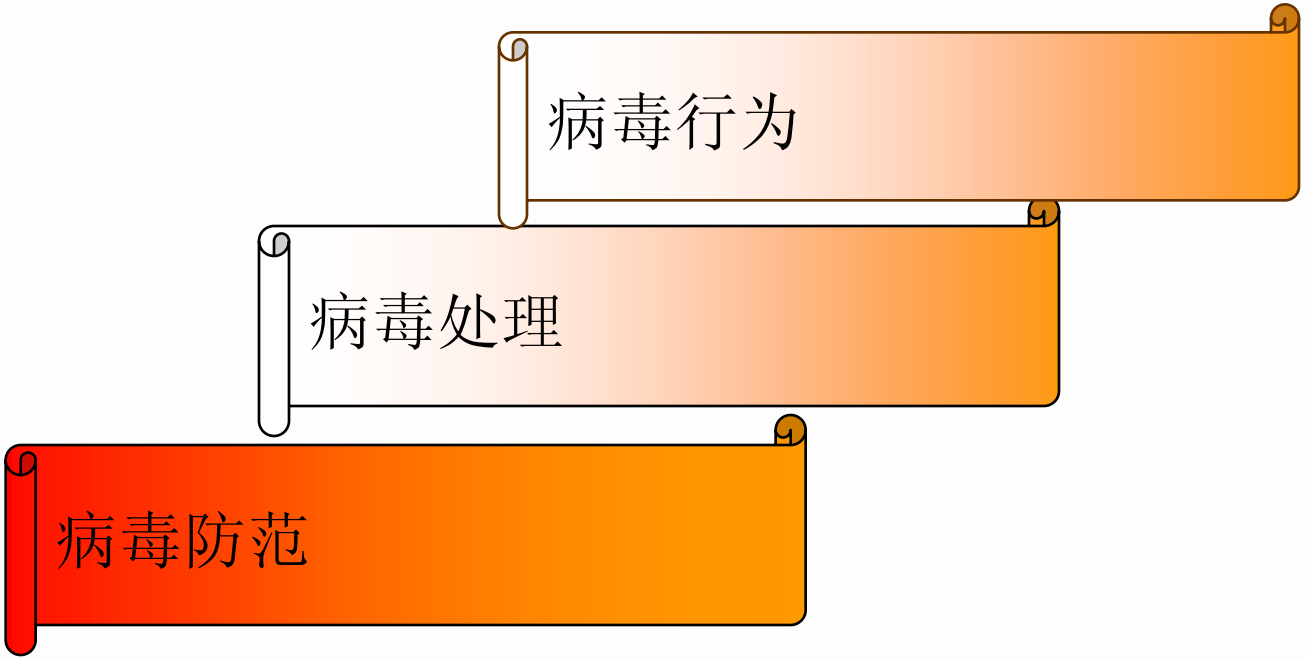
淘宝桌面快捷方式无法删除



淘宝桌面快捷方式无法删除

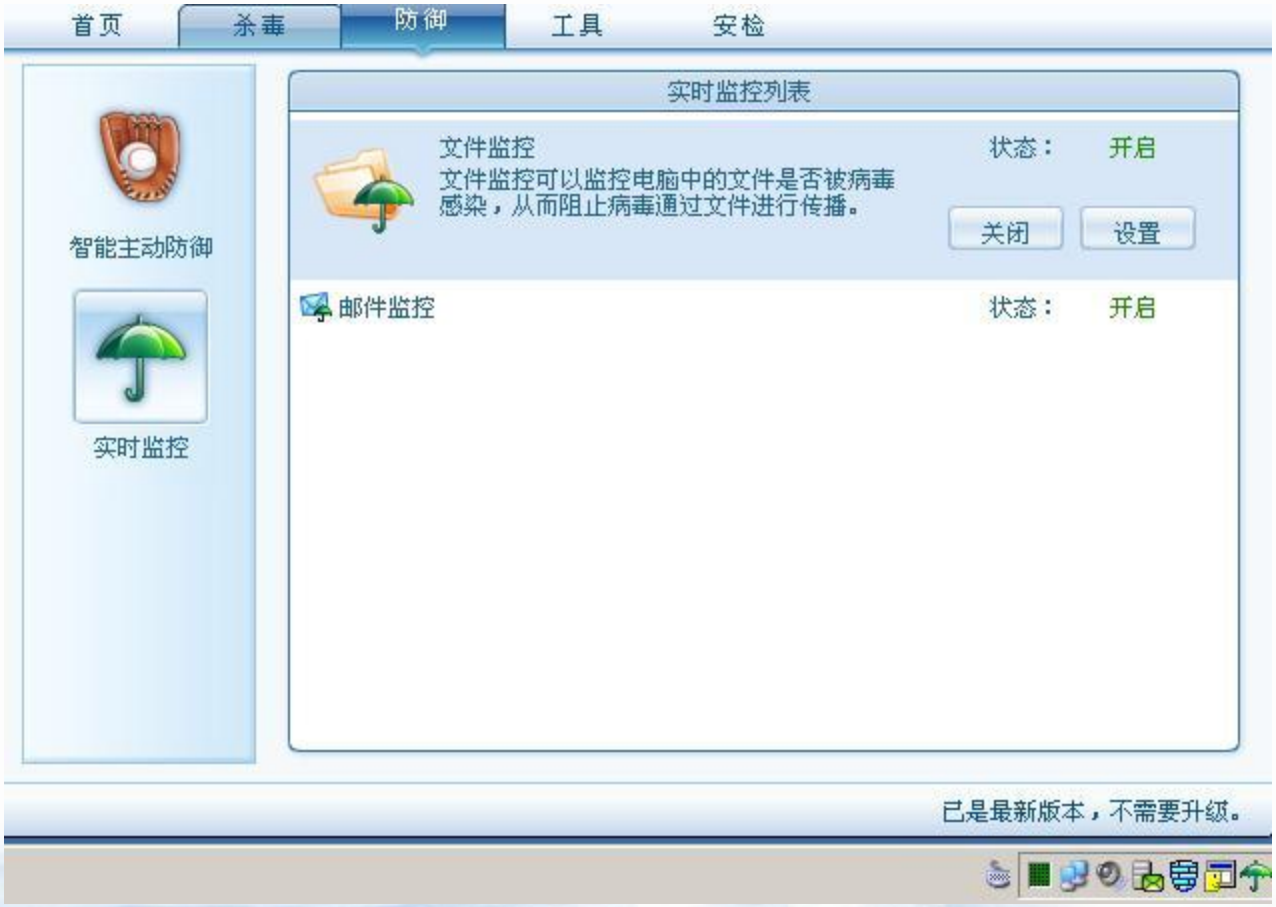
使用瑞星IE修复工具：Fix_With_ui.exe

淘宝桌面快捷方式无法删除



淘宝桌面快捷方式无法删除

保证瑞星监控正常开启，定期全盘杀毒。

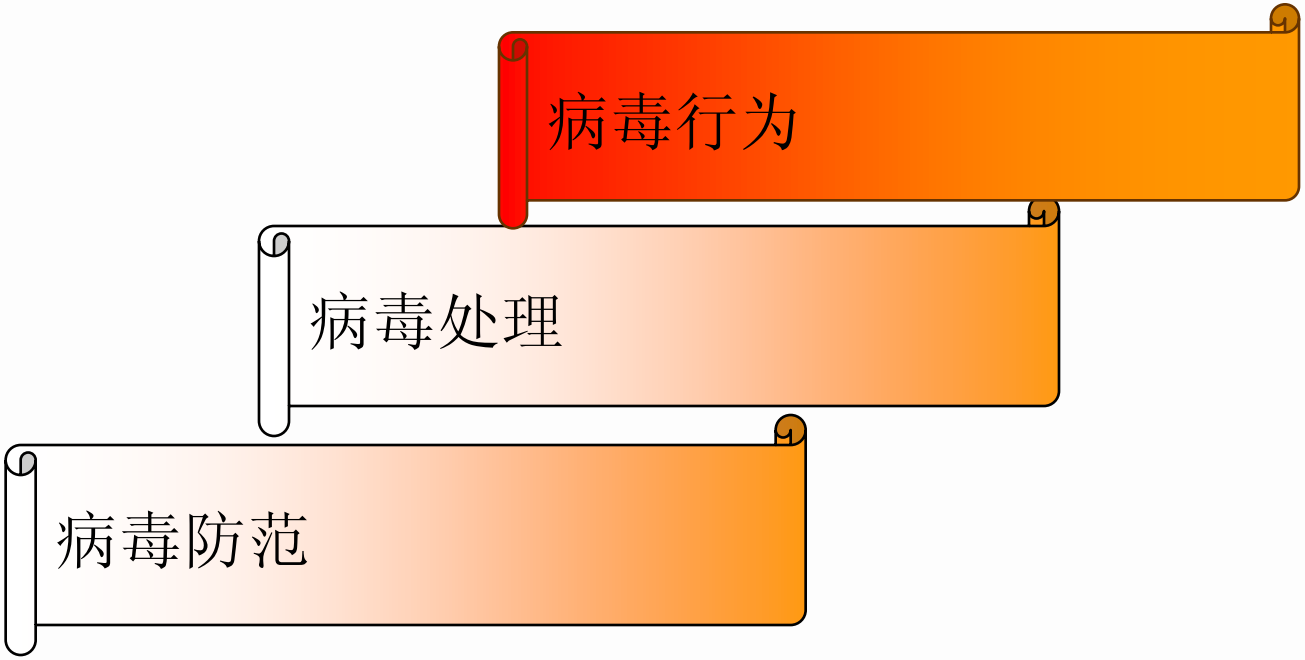


两类快捷方式类病毒的处理过程

1、淘宝桌面快捷方式无法删除

2、1KB快捷方式（暴风一号）的处理过程

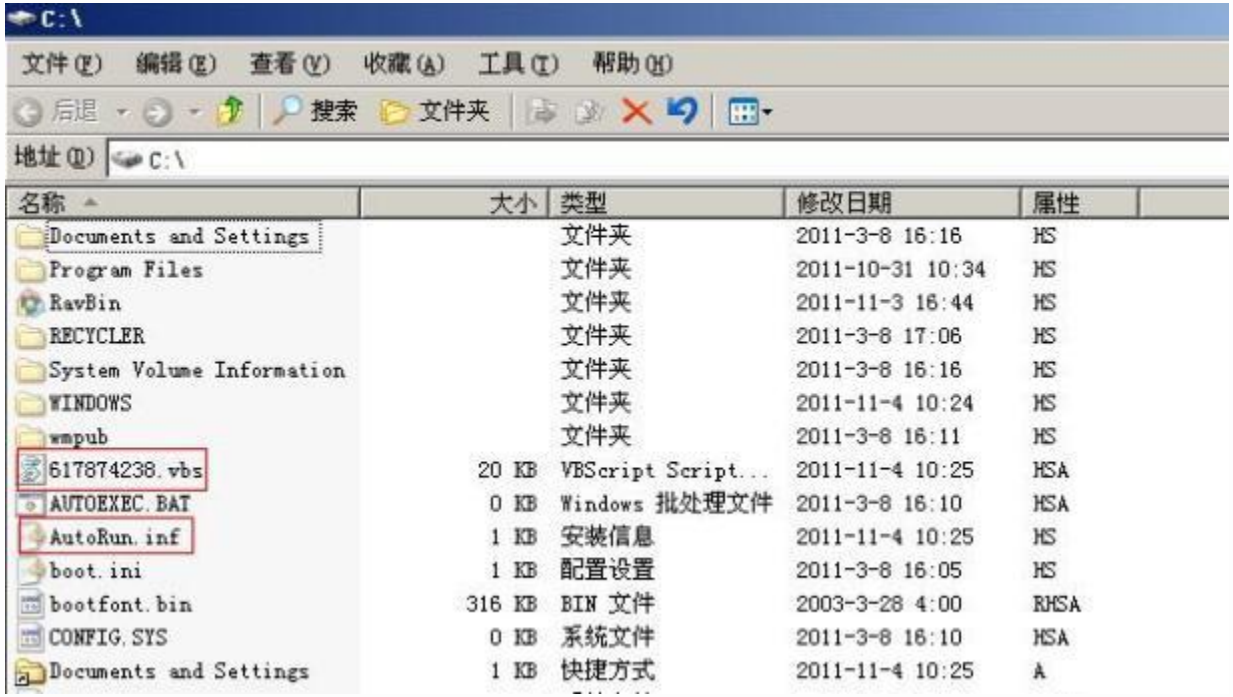
暴风一号处理过程



暴风一号处理过程

一、病毒会遍历各个磁盘，并向其根目录写入 Autorun.inf 以及 .vbs 文件，当用户双击打开磁盘时，会触发病毒文件，使之运行。

暴风一号处理过程


C:\
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) C:\
名称 大小 类型 修改日期 属性
Documents and Settings 文件夹 2011-3-8 16:16 HS
Program Files 文件夹 2011-10-31 10:34 HS
RavBin 文件夹 2011-11-3 16:44 HS
RECYCLER 文件夹 2011-3-8 17:06 HS
System Volume Information 文件夹 2011-3-8 16:16 HS
WINDOWS 文件夹 2011-11-4 10:24 HS
wmpub 文件夹 2011-3-8 16:11 HS
617874238.vbs 20 KB VBScript Script... 2011-11-4 10:25 HSA
AUTOEXEC.BAT 0 KB Windows 批处理文件 2011-3-8 16:10 HSA
AutoRun.inf 1 KB 安装信息 2011-11-4 10:25 HS
boot.ini 1 KB 配置设置 2011-3-8 16:05 HS
bootfont.bin 316 KB BIN 文件 2003-3-28 4:00 RHSA
CONFIG.SYS 0 KB 系统文件 2011-3-8 16:10 HSA
Documents and Settings 1 KB 快捷方式 2011-11-4 10:25 A

暴风一号处理过程

二、修改注册表

- 当用户运行 inf,bat,cmd,reg,chm,hlp 类型的文件，打开 Internet Explorer ，或者双击我的电脑图标时，会触发病毒文件
- 用于使文件夹选项中的“显示隐藏文件”选项失效
- 快捷方式的图标上叠加的小箭头消失
- 开启所有磁盘的自动运行特性。
- 病毒可以开机自启动

暴风一号处理过程

三、病毒会递归遍历各个盘的文件夹，当遍历到文件夹之后，会将文件夹设置为“隐藏 + 系统 + 只读”属性。同时创建一个快捷方式，其目标指向 vbs 脚本，参数指向被病毒隐藏的文件夹。由于病毒修改的注册表会使查看隐藏文件的选项失效，也会屏蔽快捷方式图标的小箭头，所以具有很大的迷惑型，让用户误以为打开的是文件夹。

暴风一号处理过程


C:\
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) C:\
名称 大小 类型 修改日期 属性
wmpub 1 KB 快捷方式 2011-11-4 10:25 A
WINDOWS 1 KB 快捷方式 2011-11-4 10:25 A
System Volume Information 1 KB 快捷方式 2011-11-4 10:25 A
rising.ini 1 KB 配置设置 2011-11-3 15:09 RHS
RECYCLER 1 KB 快捷方式 2011-11-4 10:25 A
RavBin 1 KB 快捷方式 2011-11-4 10:25 A
Program Files 1 KB 快捷方式 2011-11-4 10:25 A
pagefile.sys 589,824 KB 系统文件 2011-11-4 10:23 HSA
ntldr 298 KB 系统文件 2005-4-4 22:19 RHSA
NTDETECT.COM 47 KB 应用程序 2005-4-4 22:19 RHSA
MSDOS.SYS 0 KB 系统文件 2011-3-8 16:10 RHSA
IO.SYS 0 KB 系统文件 2011-3-8 16:10 RHSA
Documents and Settings 1 KB 快捷方式 2011-11-4 10:25 A

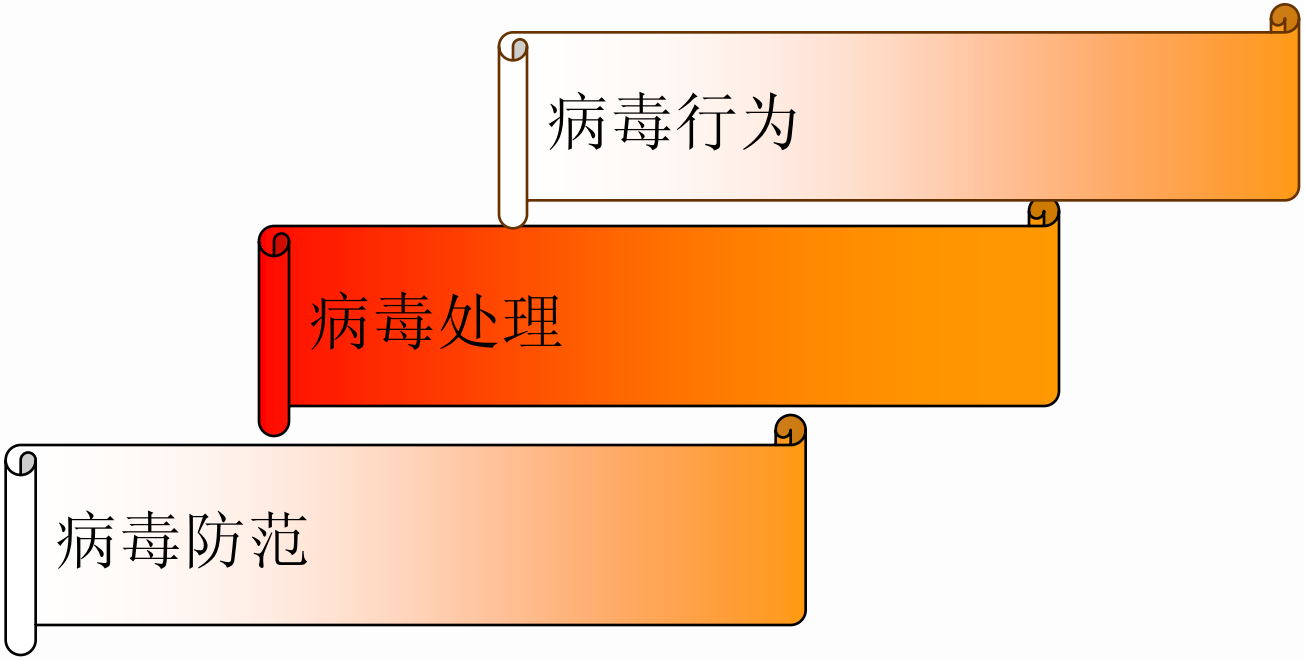
暴风一号处理过程

四、关闭弹出光驱。

五、会调用 mstha.exe 显示骷髅头图片，并且锁定计算机，使用户无法操作。

六、遍历进程，如果发现有 regedit.exe 、 taskmgr.exe 等进程，就调用 ntsd 命令结束进程，使用户无法打开注册表编辑器，和任务管理器等一些基本的系统工具。

暴风一号处理过程



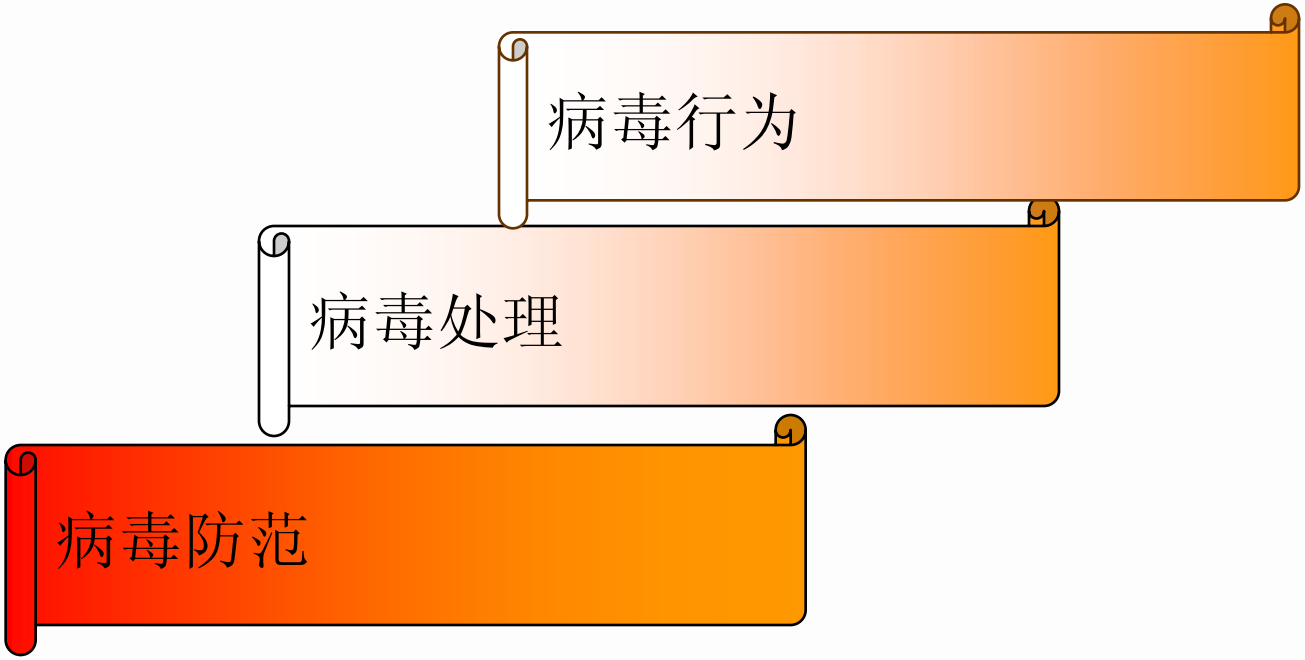
暴风一号处理过程

一、使用瑞星全盘杀毒。

二、使用专杀工具。

三、通过一些病毒处理工具处理，常见的有wsyscheck。

暴风一号处理过程



暴风一号处理过程

修改瑞星文件监控级别。

- 通过这上面的两个案例可以看出，为了更高效的处理某些病毒，可以适当采用专杀工具，那么瑞星网络版对我们的网络安全带来哪些帮助那？

瑞星对网络安全的帮助

瑞星对网络安全的帮助

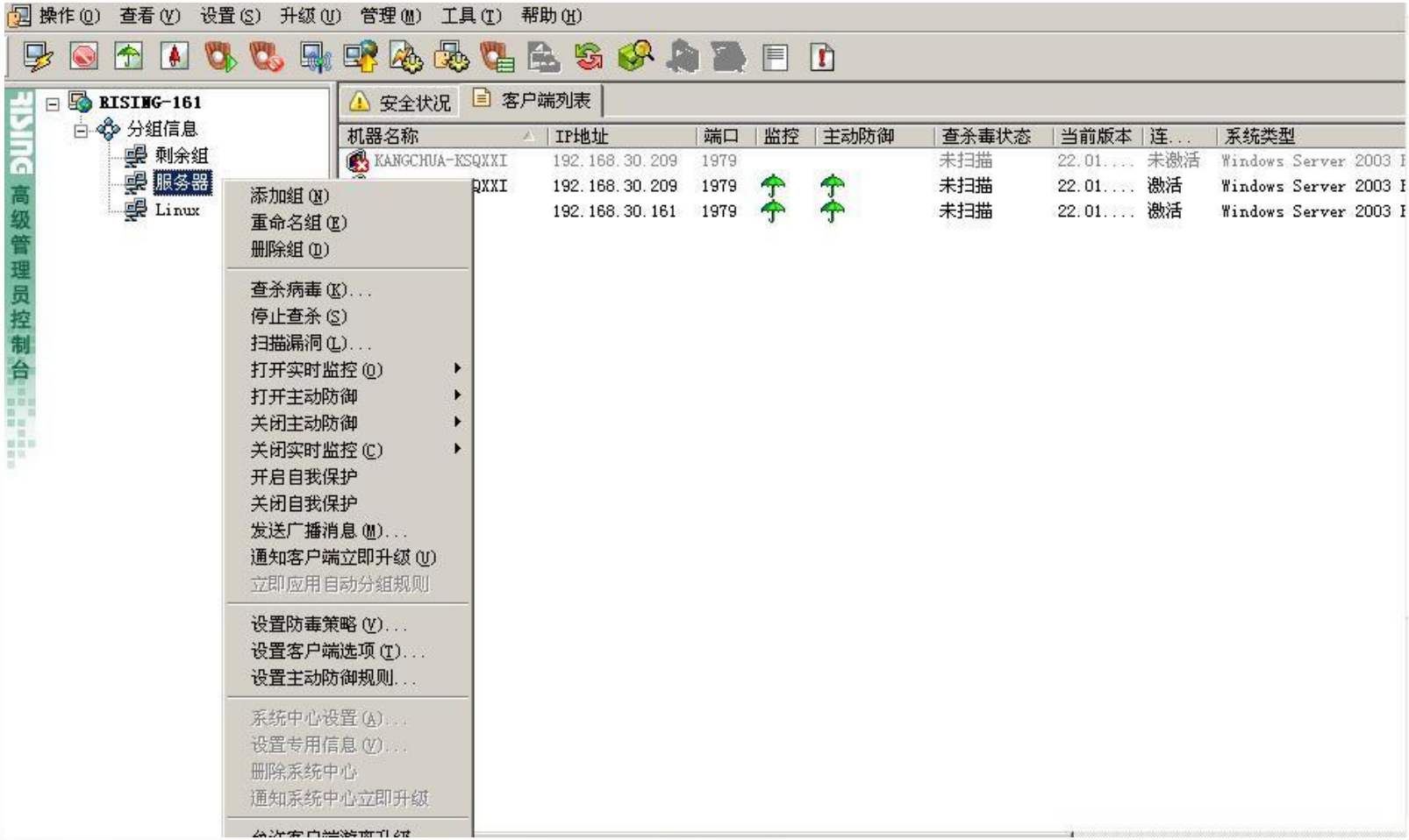
1、全网制订统一的安全策略

2、快速有效的定位网络中病毒并处理

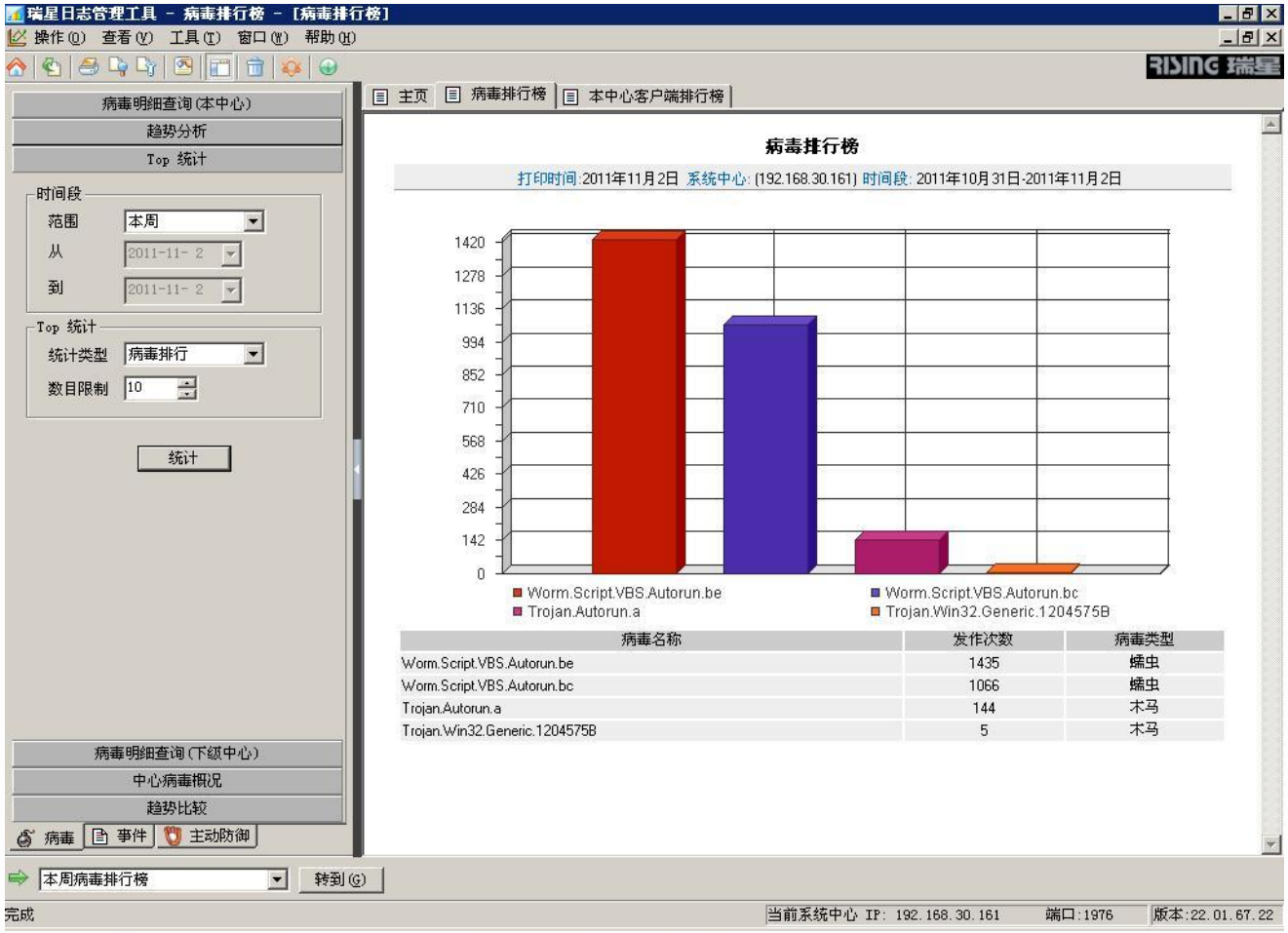
3、防范移动设备随意接入内网

4、及时发现系统漏洞并自动分发补丁

全网制订统一的安全策略

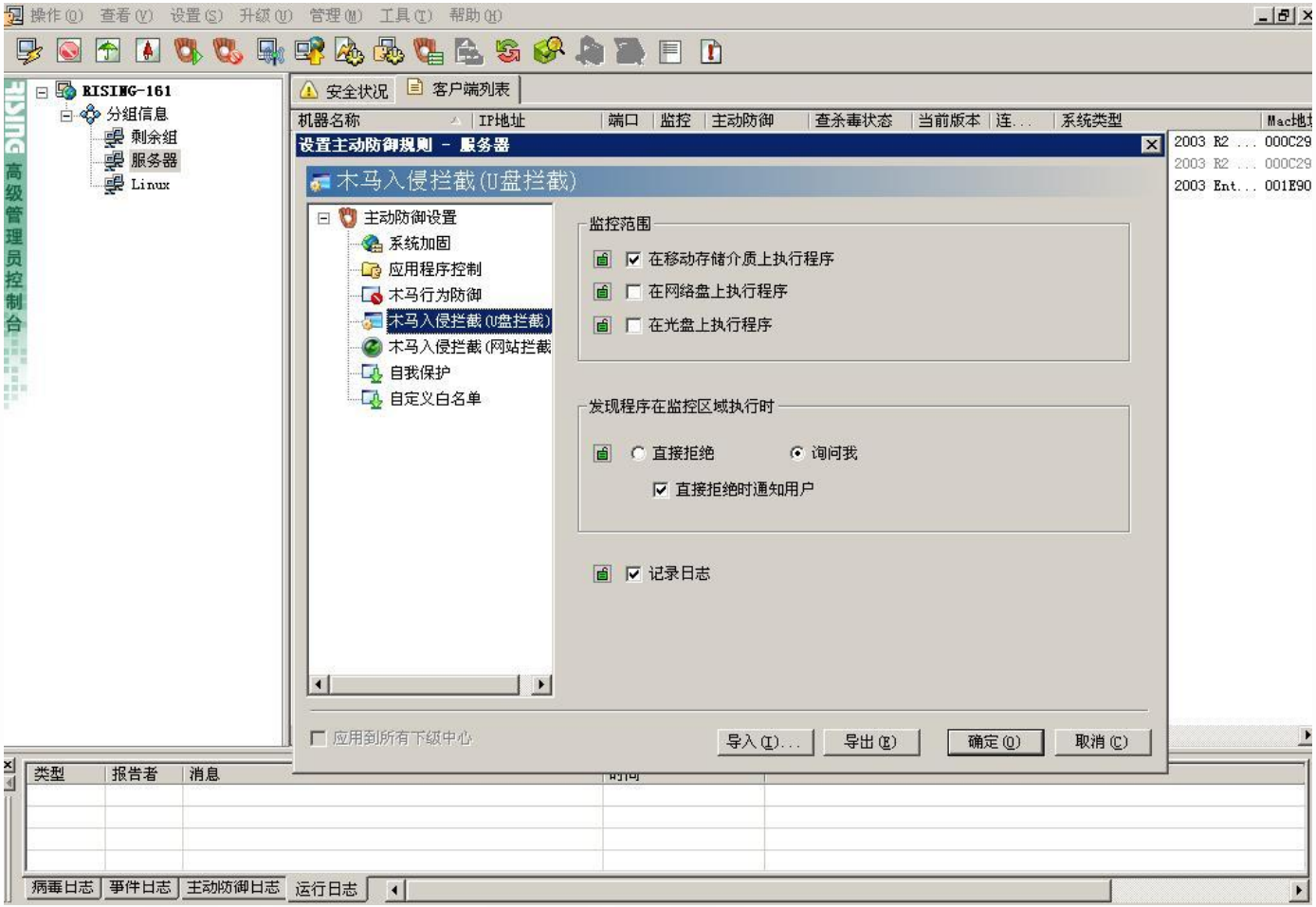


快速有效的定位网络中病毒并处理

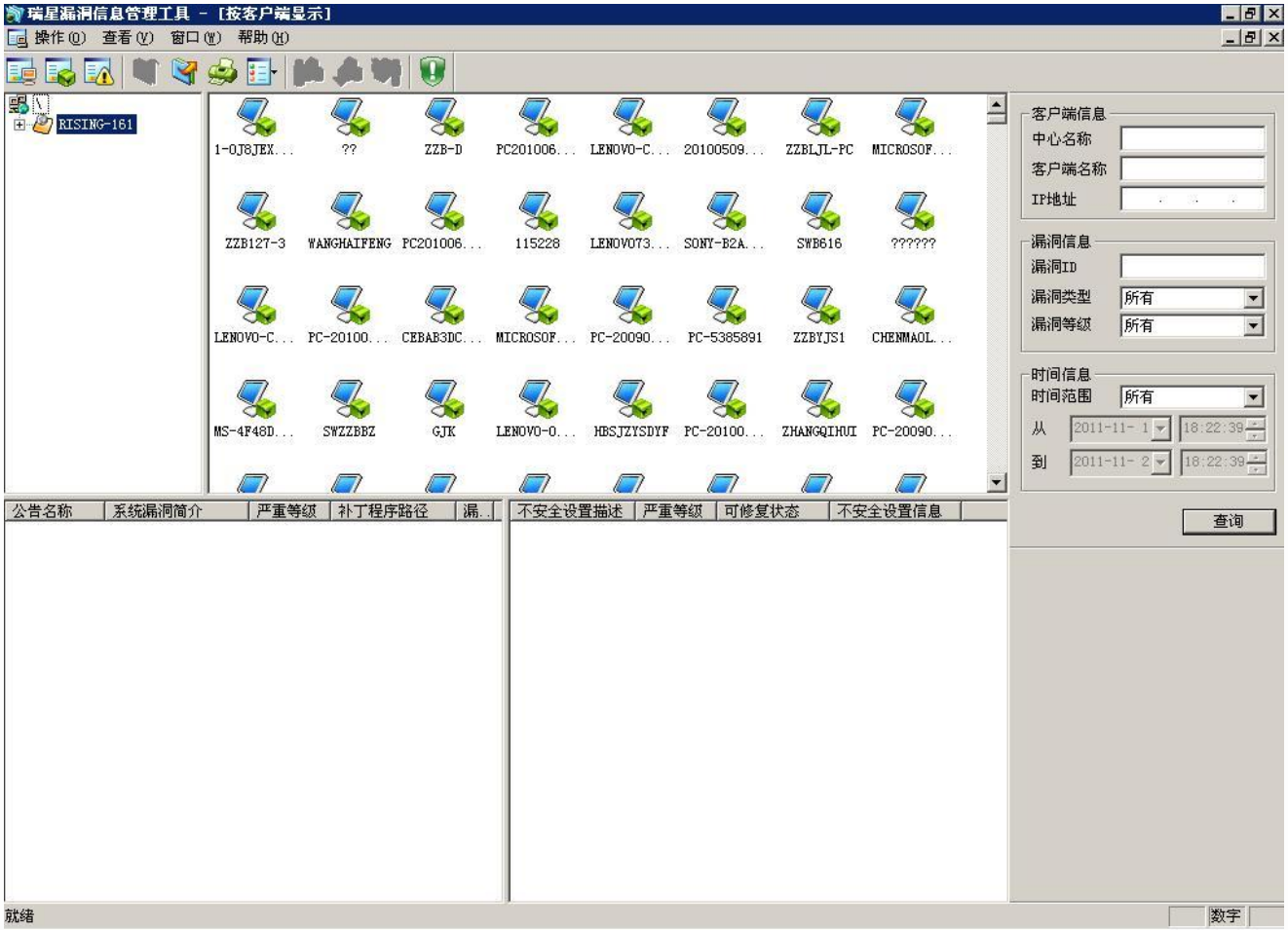


RISING 瑞星

防范移动设备随意接入内网



及时发现系统漏洞并自动分发补丁



易忽略的瑞星网络版实用功能

易忽略的瑞星网络版实用功能

1、远程修复可以解决大多数问题

2、由于补丁下载过多，导致C盘空间不足了怎么办

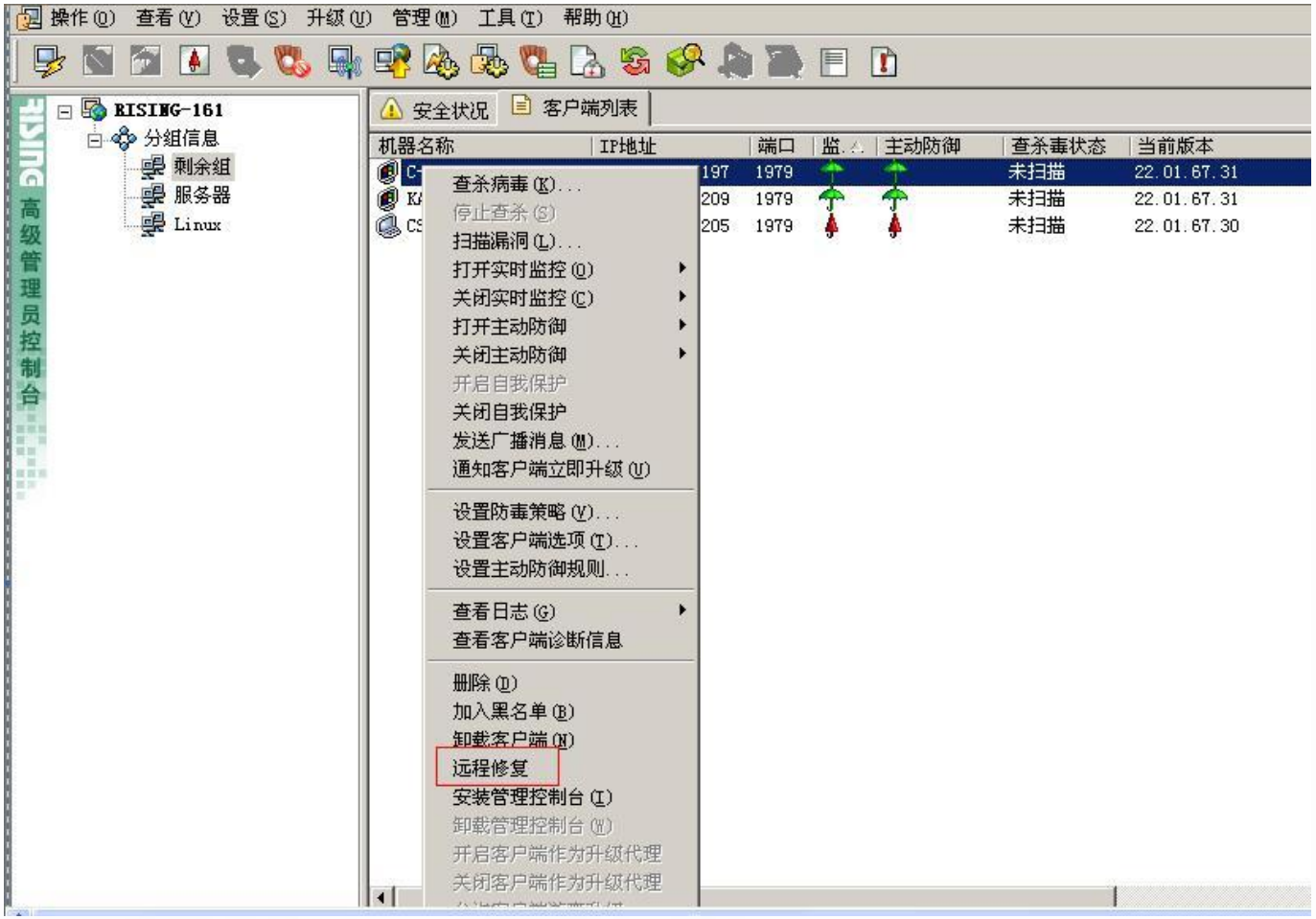
3、统一不要瑞星小狮子

4、网内客户端较多，升级造成中心负荷过大

5、客户端安装包制作工具

6、便捷的分组规则管理

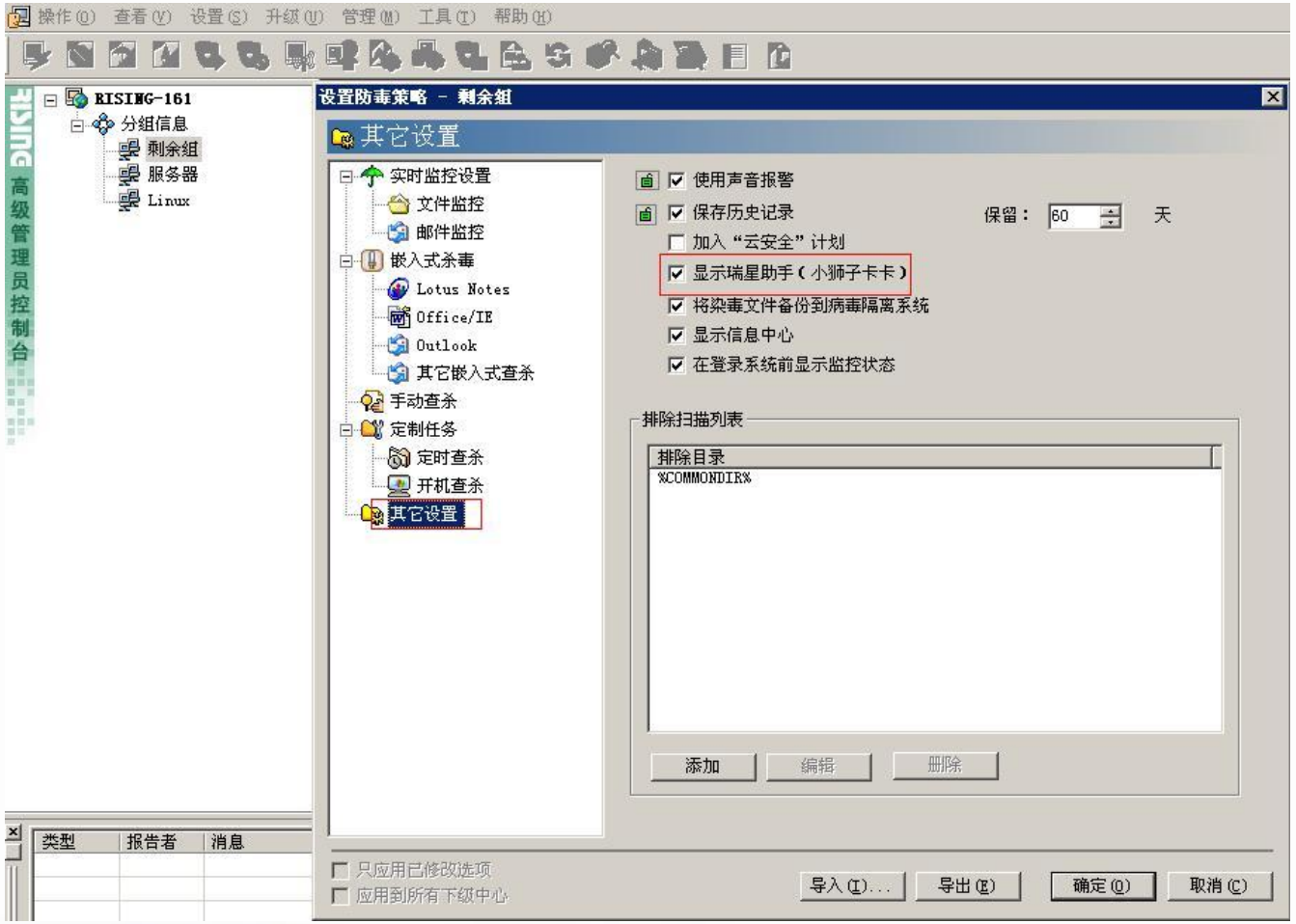
远程修复可以解决大多数问题



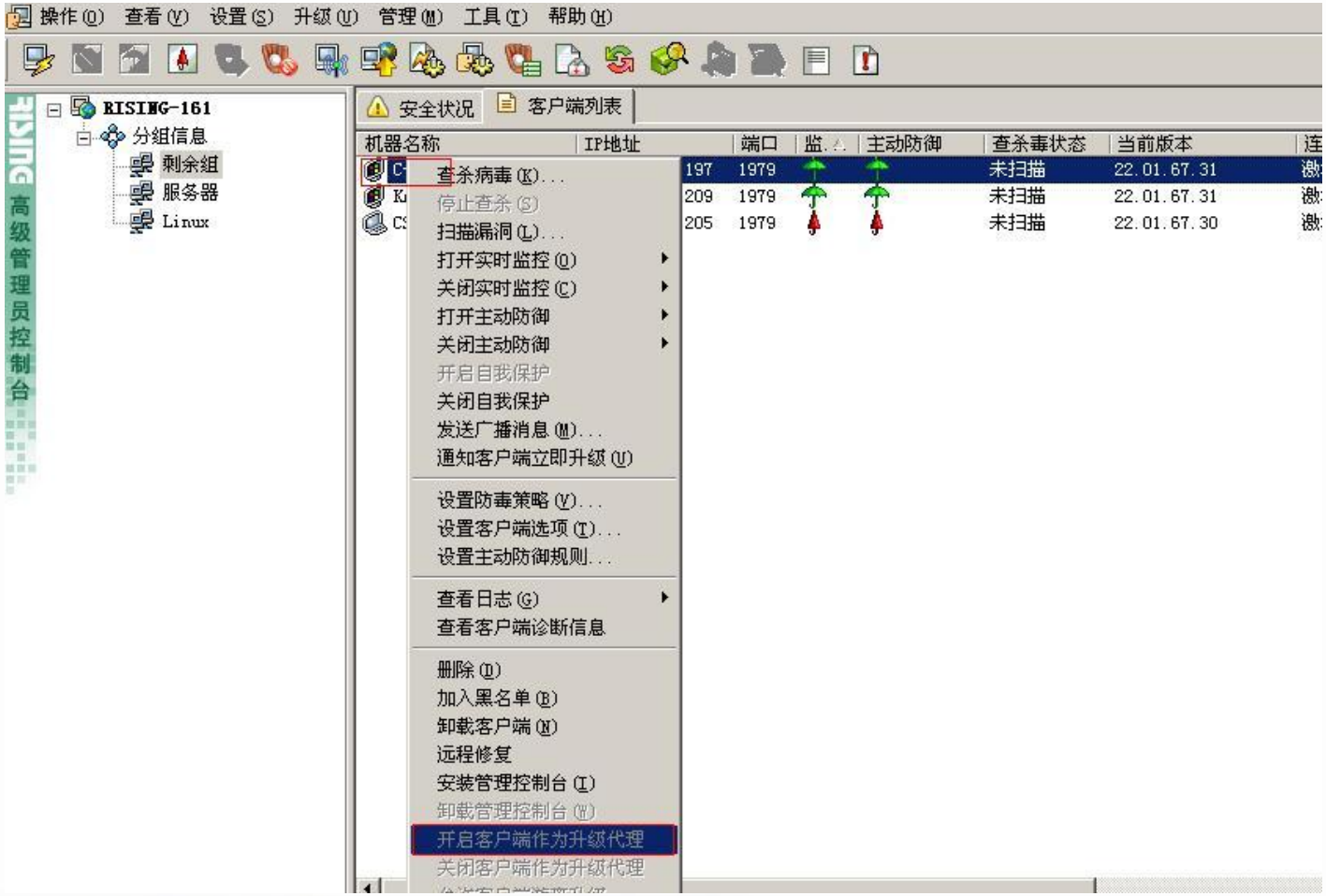
C盘空间不足


瑞星漏洞信息管理工具 - [按客户端显示]
操作(O)
查看(V)
窗口(W)
帮助(H)
通知瑞星下载中心下载补丁程序(H)
通知安装补丁程序(C)
通知修复不安全设置(N)
系统漏洞详细信息(K)...
不安全设置详细信息(S)...
导出数据(E)...
选项(O)
设置新的补丁程序存放路径(N)...
打印(P)... Ctrl+P
退出(X)

统一不要瑞星小狮子


操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
RISING-161
分组信息
剩余组
服务器
Linux
高级管理员控制台
设置防毒策略 - 剩余组
其它设置
实时监控设置
文件监控
邮件监控
嵌入式杀毒
Lotus Notes
Office/IE
Outlook
其它嵌入式查杀
手动查杀
定制任务
定时查杀
开机查杀
其它设置
使用声音报警
保存历史记录
保留: 60 天
加入“云安全”计划
显示瑞星助手(小狮子卡卡)
将染毒文件备份到病毒隔离系统
显示信息中心
在登录系统前显示监控状态
排除扫描列表
排除目录
%COMMONDIR%
添加
编辑
删除
只应用已修改选项
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)
类型
报告者
消息

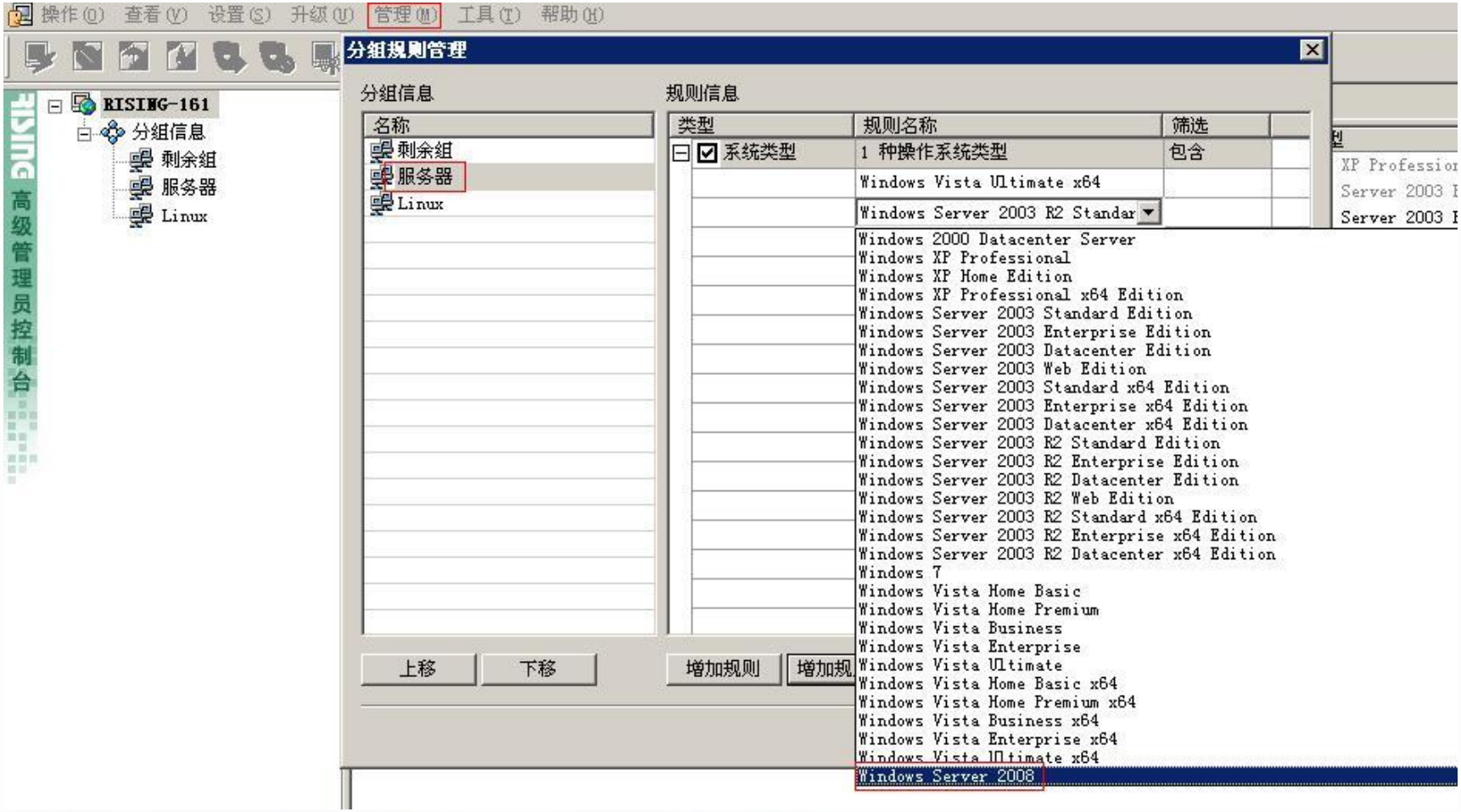
升级造成中心负荷过大


操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
RISING-161
分组信息
剩余组
服务器
Linux
安全状况
客户端列表
机器名称
IP地址
端口
监...
主动防御
查杀毒状态
当前版本
197 1979 未扫描 22.01.67.31
209 1979 未扫描 22.01.67.31
205 1979 未扫描 22.01.67.30
查杀病毒(K)...
停止查杀(S)
扫描漏洞(L)...
打开实时监控(O)
关闭实时监控(C)
打开主动防御
关闭主动防御
开启自我保护
关闭自我保护
发送广播消息(M)...
通知客户端立即升级(U)
设置防毒策略(Y)...
设置客户端选项(T)...
设置主动防御规则...
查看日志(G)
查看客户端诊断信息
删除(D)
加入黑名单(B)
卸载客户端(N)
远程修复
安装管理控制台(I)
卸载管理控制台(W)
开启客户端作为升级代理
关闭客户端作为升级代理
RISING 高级管理员控制台

客户端安装包制作工具


管理控制台
企业管理器
下载中心管理工
记事本
系统中心数据备
客户端配置工具
所有程序(P)
开始
XueTr
附件
谷歌浏览器
管理工具
弘远4S店客户关系管理系统
启动
全能工具箱
瑞星安全游戏
瑞星个人防火墙
瑞星杀毒软件网络版
瑞星远程服务系统工程师端
豌豆荚手机精灵
HyperSnap 6
Mozilla Firefox
Windows Search
Internet Explorer
瑞星工具
瑞星网站
病毒隔离区
管理控制台
漏洞信息管理工具
瑞星监控中心
瑞星日志管理工具
瑞星杀毒软件网络版
添加删除组件
RavID重置工具
分组导入工具
客户端安装包打包工具
客户端配置工具
客户端搜索工具
嵌入式杀毒设置
日志打包工具
瑞星快捷方式查杀
瑞星助手
系统中心数据备份工具
下载中心管理工具

便捷的分组规则管理


操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
RISING 高级管理员控制台
RISING-161
分组信息
剩余组
服务器
Linux
分组规则管理
分组信息
规则信息
名称
剩余组
服务器
Linux
类型
规则名称
筛选
系统类型
1 种操作系统类型
包含
Windows Vista Ultimate x64
Windows Server 2003 R2 Standar
Windows 2000 Datacenter Server
Windows XP Professional
Windows XP Home Edition
Windows XP Professional x64 Edition
Windows Server 2003 Standard Edition
Windows Server 2003 Enterprise Edition
Windows Server 2003 Datacenter Edition
Windows Server 2003 Web Edition
Windows Server 2003 Standard x64 Edition
Windows Server 2003 Enterprise x64 Edition
Windows Server 2003 Datacenter x64 Edition
Windows Server 2003 R2 Standard Edition
Windows Server 2003 R2 Enterprise Edition
Windows Server 2003 R2 Datacenter Edition
Windows Server 2003 R2 Web Edition
Windows Server 2003 R2 Standard x64 Edition
Windows Server 2003 R2 Enterprise x64 Edition
Windows Server 2003 R2 Datacenter x64 Edition
Windows 7
Windows Vista Home Basic
Windows Vista Home Premium
Windows Vista Business
Windows Vista Enterprise
Windows Vista Ultimate
Windows Vista Home Basic x64
Windows Vista Home Premium x64
Windows Vista Business x64
Windows Vista Enterprise x64
Windows Vista Ultimate x64
Windows Server 2008
上移
下移
增加规则
增加规
XP Professio
Server 2003
Server 2003

感谢您的参与！
您的观点，我们用心倾听