# 瑞星之剑勒索病毒防御软件产品介绍

## 一、背景

随着信息化的发展数据安全成为信系技术最重要的领域之一，特别是数据内容的防篡改，完整性保护方面的功能需求更加迫切，近年来许多恶意软件作者把目标针对用户文档，对用户文件进行加密和篡改，进行恶意敲诈，特别是最近的永恒之蓝漏洞爆发而广为传播的wanncry类的勒索病毒更是给国家和社会造成了重大损失。

传统杀毒软件目前对文档破环类的勒索病毒没有特别好的处理方式，只能在发现病毒后进行病毒处理，而已经被病毒加密和篡改的文档无法恢复和处理，用户只能够寄希望与先前备份过这些资料和数据，无法进行先期防御。各大厂商的关端口，打补丁等应急方案智能解一时之急，不仅影响现有业务系统，而且无法防御将来通过其他途径传播的病毒。

瑞星团队为打破防御勒索病毒的被动局面，第一时间研制出瑞星之剑，一款能防御未知勒索病毒的安全产品。

## 二、技术原理

### 智能诱饵

瑞星之剑会在用户桌面，文档，图片等关键目录释放文档，图片等类型的诱饵文件。当检测到疑似勒索病毒篡改/删除诱饵文件，及时隔离可疑进程，防止用户其他重要文件被加密。

### 文件格式检测

瑞星之剑通过监控用户的文档，图片，数据等类型的文件，当检测到文件文件内容被修改时，读取文档原有内容，进行文档格式识别，并根据写入的文档的内容再次进行文档格式识别，判断如果修该完成用户的文档格式是否被篡改，如果被篡改直接通知监控模块拒绝这次修改，并及时隔离可疑进程。

### 勒索病毒行为分析

瑞星通过对近年来勒索病毒家族的分析，总结出勒索病毒若干行为特征：

1. 遍历用户关键目录，如我的文档，图片，桌面
2. 篡改/删除 文档，图片等重要文件
3. 创建未知格式的加密文件
4. 生成勒索提示文件

当检测到可疑程序文件操作序列包含但不限于以上特征时，及时隔离可以进程。

## 三、应用环境

|  |  |  |
| --- | --- | --- |
| Windows系统 | 32bit | Xp |
| 2003 |
| Win7 |
| Vista |
| win8 |
| Win8.1 |
| 2008 |
| 2012 |
| Win10 |
| 64bit | Xp |
| 2003 |
| Win7 |
| Vista |
| win8 |
| Win8.1 |
| 2008 |
| 2012 |
| Win10 |

“瑞星之剑勒索病毒防御软件”采用快速安装方式，省去安装流程，工具启动后直接创建相应服务，进程，驱动，开启保护。

## 四、开始使用

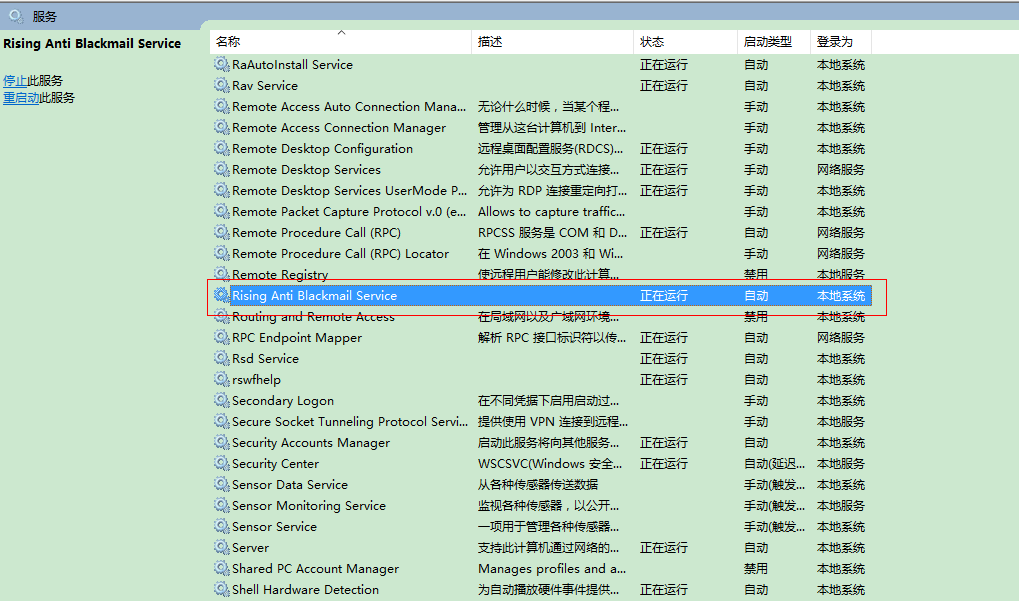
双击“瑞星之剑勒索病毒防御软件”（rsbmterm.exe）启动软件。

1)启动后“瑞星之剑勒索病毒防御软件”主程序打开，该界面显示软件已处于保护状态。界面中包含软件版本信息，提供设置功能，检查更新功能



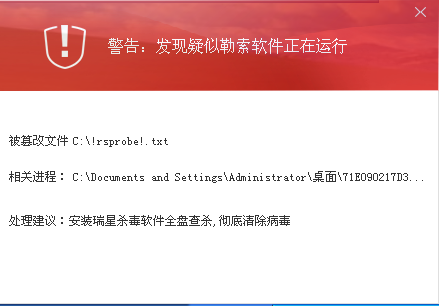
2)托盘程序打开。系统任务栏托盘区域显示“瑞星之剑勒索病毒防御软件”托盘图标，表示软件已启动。鼠标左键单击托盘图标会打开主程序界面，鼠标右键单击图标，显示退出按钮

3)软件服务开启。



## 五、拦截提示

“瑞星之剑勒索病毒防御软件”运行过程中，软件会实时监控进程的启动和运行，一旦发现有已知或未知的勒索病毒运行，软件会自动弹出提示框提醒使用者注意风险，并依据使用者的设置进行自动或非自动处理勒索病毒进程。



提示框内容

被篡改的文件：显示勒索病毒正在感染的文件，以全路径形式展示

相关进程：显示勒索病毒的进程信息，勒索病毒所在位置

处理建议：建议使用者发现有勒索病毒后及时安装瑞星杀毒软件进行全盘查杀，提高防护能力。