主动防御

田庆亮

2011年9月9日

主要内容

- 主动防御介绍
- Hips介绍
- 瑞星主动防御
- 产品问题答疑

主动防御

主动防御是基于程序行为自主分析判断的实时防护技术，不以病毒的特征码作为判断病毒的依据，而是从最原始的病毒定义出发，直接将程序的行为作为判断病毒的依据。

主动防御特点

- 创立动态仿真反病毒检测系统
- 自动准确判定新病毒
- 程序行为监控并举
- 自动提取特征值实现多重防护

主动防御的主要技术

- 一是在未知病毒和未知程序方面，通过先进的“行为判断”技术，提供“危险行为监控”、“行为自动分析和诊断”等检测和监控服务。
- 二是先进的智能分析系统，将对漏洞攻击行为进行监测，防止病毒利用系统漏洞对其它计算机进行攻击，从而阻止病毒的植入等等。

HIPS

- HIPS主机入侵防御系统，目前广泛称作系统防火墙，是一种通过拦截系统内软件的常见危险动作，借助相应人为或软件内的触发条件制止一些不正常的软件动作，以达到系统安全的一个软件。

纯手动HIPS

- 纯手动HIPS，就是在极端情况下（安装好HIPS类软件后，删除内置的规则或者不开启学习模式），所有的操作都要有用户的参与，才能完成。之所以这类HIPS会受到很多高手的青睐，就是因为利用它们，可以基本做到对自己电脑的完全控制，这种完全控制的感觉更加能够让人获得心理上的满足和愉悦。

瑞星智能主动防御

- 瑞星智能主动防御 
- 瑞星的主动防御技术提供了更开放的高级用户自定义规则的功能，用户可以根据自己系统的特殊情况，制定独特的防御规则，使主动防御可以最大限度的保护系统。

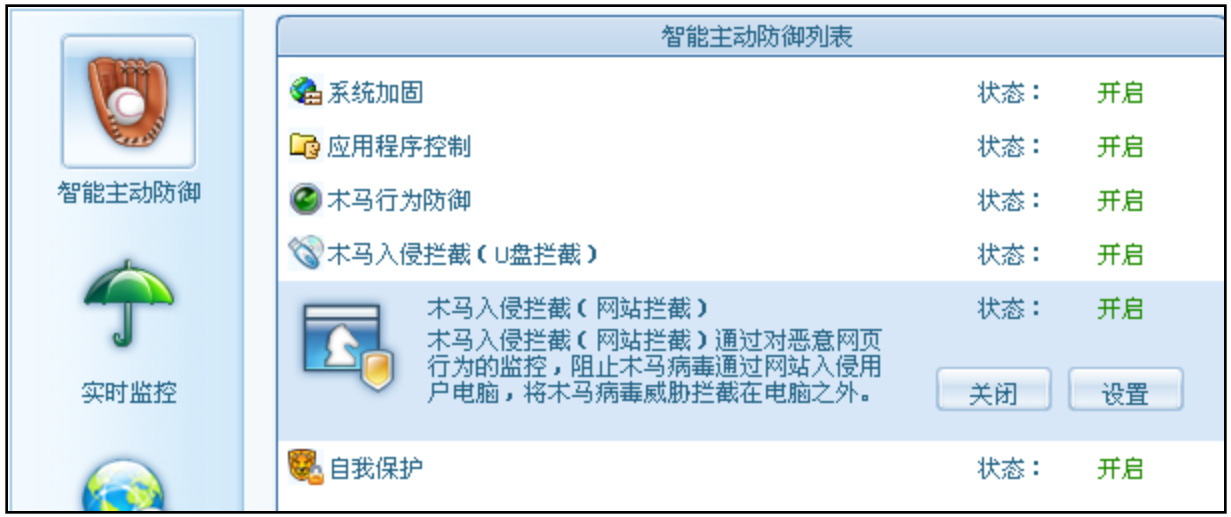
瑞星主动防御与HIPS的关系

简单来说瑞星的主动防御就是定制版的HIPS，HIPS是你自己创建规则，凡触犯规则的都会进行拦截，而主动防御是监控软件的行为，如果行为触犯了病毒的行为特征就会报毒。

一个是纯手工，一个是智能判断，两种方式如果单纯只针对功能做比较的话，HIPS比较安全，但对用户技术要求极高，而主动防御比较方便，非常适合普通用户使用。

瑞星智能主动防御

- 瑞星主动防御由系统加固、应用程序控制、木马行为防御、木马入侵拦截（U盘拦截）、木马入侵拦截（网站拦截）和自我保护等功能组成。



系统加固

- 系统加固针对恶意程序容易利用的操作系统脆弱点进行监控、加固，以抵御恶意程序对系统的侵害。
- 系统加固对系统动作、注册表、关键进程和系统文件进行监控，从而防止恶意程序对操作系统进行修改系统进程，操作注册表，破坏关键进程和系统文件等危险行为。

系统加固

- 系统加固设置


系统加固
系统监控
注册表监控
关键进程保护
系统文件保护
本类所有规则
系统动作监控
挂全局钩子
修改内核内存数据
加载驱动程序
修改系统日期及时间
关闭电脑
使用摄像头
安装驱动
底层磁盘访问
系统监控将及时发现并拦截系统异常的加载和访问调用，最大限度地保证系统运行的安全和稳定。
确定(O)
取消(C)
应用(A)

应用程序控制

- 应用程序控制允许用户对监控设置进行个性化定义，来监控程序的运行状态，拦截进程的异常行为，为用户提供个性化的保护。
- 此功能是由用户先进行设置，选择指定的进程，选择适合的模板，设置完毕后，当开启此功能时候，应用程序控制的功能生效。

应用程序控制

- 应用程序控制设置

木马行为防御

- 通过对木马等病毒的行为分析，智能监控未知木马等病毒，抢先阻止其偷窃和破坏行为。
- 此功能是瑞星网络版客户端软件提供内置规则，用户可以进行相关设置，当开启此功能时候，木马行为防御功能生效。

木马行为防御

- 木马行为防御设置

木马入侵拦截（U盘拦截）

- 通过对木马病毒传播行为的分析，阻止其通过U盘、光盘等入侵用户电脑，阻断其利用存储介质传播的通道。
- 木马入侵拦截（U盘拦截）取代了原来的U盘监控，控制范围更广，能够更好地控制执行区域，避免外部病毒感染到主机。当木马入侵拦截（U盘拦截）范围内的程序试图自动运行或直接运行的时候，进行拦截，并提示用户。

木马入侵拦截（U盘拦截）

- 木马入侵拦截（U盘拦截）设置

木马入侵拦截（网站拦截）

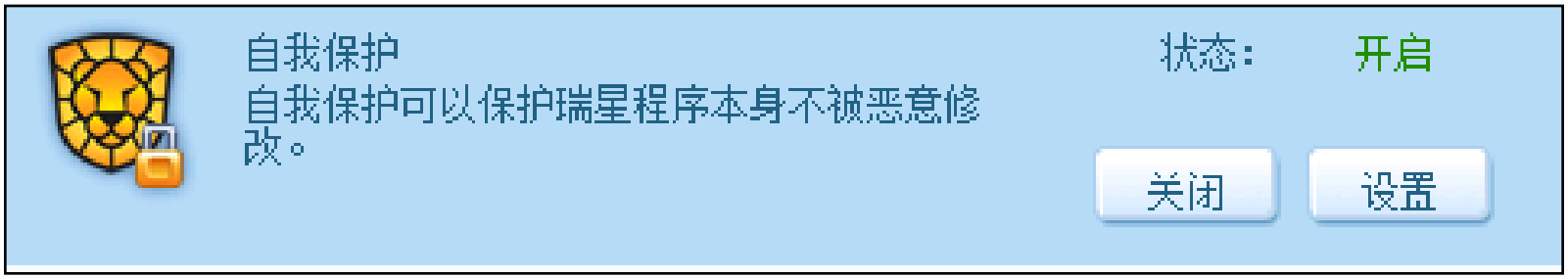
- 通过对恶意网页行为的监控，阻止木马病毒通过网站入侵用户电脑，将木马病毒威胁拦截在电脑之外。
- 木马入侵拦截（网站拦截）突破了原来网页脚本扫描只能通过特征进行查杀的技术壁垒。解决了原网页脚本监控无法对加密变形的病毒脚本进行处理的问题。

木马入侵拦截（网站拦截）

- 木马入侵拦截（网站拦截）设置

自我保护

- 瑞星网络版客户端软件提供自我保护功能，防止恶意程序破坏瑞星网络版客户端软件。如果有破坏瑞星网络版客户端软件的情况出现，电脑右下方会有相应提示。



常见产品问题

- 产品问题解答


谢谢大家