智恒恶意代码辅助检测系统V4.0

产品名称	智恒恶意代码辅助检测系统V4.0
公司名称	北京利源嘉志科技有限责任公司
价格	5500.00/套
规格参数	品牌:智恒 型号:V4.0 产地:北京
公司地址	北京市海淀区阜成路14号
联系电话	15110266611

产品详情

智恒恶意代码辅助检测系统技术实现原理

TrojanChecker V3.0系统采用CRC、Sign智能分析和特征码相结合的技术，在协议层和系统层进行协议分析和特征追踪。

实现原理：

l 系统采用循环冗余检测方法，通过CRC算法，对系统协议、所有文件进行检错，其特点是检测能力强、系统资源占用率低。是新一代的检测技术。

l 特征码匹配技术，检测系统将协议和文件进行解析后与实现提取的恶意程序特征相匹配，从中发现攻击行为。

l 系统采用Sign技术进行辅助检测，Sign技术与系统层和应用层相结合，在操作系统底层和应用层进行关联分析，对系统文件、端口、服务、进程、应用插件等进行关联分析，从中发现未知程序。

恶意代码辅助检测系统功能特点

智能行为分析技术+特征码匹配技术，监控系统运行状况，结合病毒行为库，检测已知、变种和未知程序。

独创Trojan Seeker恶意程序分析技术，快速获取目前新的恶意程序特征。主动搜索新恶意程序。

独创Honeynet恶意程序分析技术，提供被动的方式搜集恶意程序特征。

使用CRC，Sign，特征码等方法保证检测的可靠性，大限度降低漏报误报。

设计稳定，高效的检测引擎，自动根据检测目标主机性能调节检测能力，不会对系统造成巨大的性能影响。

独特的多种检测工具相结合的方式，保证检测的可靠性

恶意代码辅助检测系统主要功能

支持超过百万级恶意程序分析，并且有的分析团队，使用新的技术每天实时分析更新新特征库。

为了保证检测的准确性，可靠性等，恶意程序分析，挖掘团队保持数据库的随时更新。

扫描引擎对所选的文件以及该文件的操作进行恶意程序检测，所有被检测到感染恶意程序的文件都将被报告，并且根据策略执行操作。

恶意程序通常被定义为恶意软件，他通常在用户不知情的情况下从用户计算收集敏感数据信息。扫描引擎将对这些恶意程序进行扫描检测，找出其中的木马程序或文件。

提供自定义恶意程序扫描方式

除了文件检测，还支持压缩文件，脚本文件检测等。

对于一些经过变种的恶意程序，提供识别能力。

提供BHO，SPI等项目的监测，查找可能被插入的代码程序。

提供报表管理中心，可以根据需要制定报表

进程监控，发现被修改或者隐藏的进程或线程。

提供恶意程序的概要特征

提供恶意程序手工清除方法

提供详细的数据分析与报表功能。

提供告警，可以在时间通知管理员。

提供高效可靠的扫描机制，在扫描的同时也不会消耗过多的系统资源。

程序运行稳定可靠，大限度降低系统漏报误报率。

对于一些可疑程序，或者网络行为，用户可以自己使用系统提供的辅助检测工具进行分析，检查是否有可疑的潜在危险。比如检查系统服务，启动项等。

系统设计采用模块化的方式，方便扩展。

支持多个策略管理，策略设置支持即时生效；

系统全中文界面，操作、配置方便，网络管理人员仅需五分钟即可熟练完成系统初始配置，大大提高工作效率；

支持软件运行状态记录，并实时记入日志，支持导出报表；

自身操作审计日志记录，详细记录操作管理员的操作管理行为；

规则库支持本地升级功能；