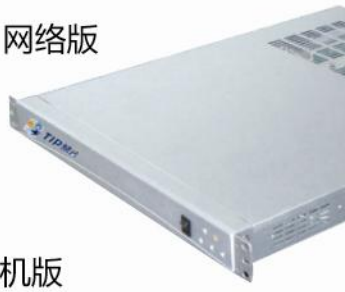
TIPS鼎普

猎隼恶意程序辅助检查系统

网络版



单机版

中国信息防泄漏领航企业

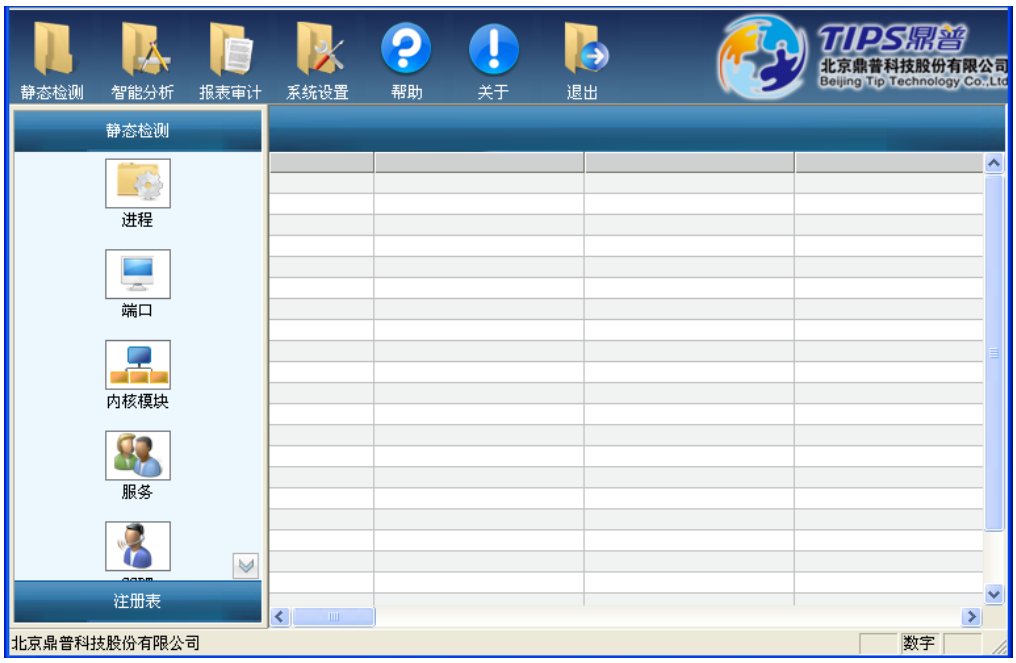
目 录

产品概述 1
产品功能 2
产品优势 3
关于鼎普 3

产品概述

木马是由攻击者安装在受害者计算机上秘密运行并窃取信息及远程控制的程序，是信息化时代信息传播者的另类载体。木马对网络信息安全造成严重危害和威胁，是引发拒绝服务攻击，造成个人、企业及国家秘密失泄漏的重要因素；据国家计算机网络应急技术处理协调中心（CNCERT）抽样监测统计，2008 年我国境内感染木马控制端的 IP 地址达到 438，386 个，感染木马被控制的 IP 地址达到 565，605 个，发送立即邮件 106 次、实施信息窃取操作 373 次。国家保密局更是把“对互联网的保密检查、对特种木马的检测”作为当前保密科技研究及保密检查工作中需要关注的重点方向。鼎普科技积极跟踪市场需求、木马技术发展形势和国家相关政策，自主研发了猎隼恶意程序辅助检查系统。

猎隼恶意程序辅助检查系统，分别以光盘+key 与防病毒 U 盘两种方式为载体，非常适合保密检查部门用于开展对涉密主机日常的安全检查工作。用于检查或自查辖区内的涉密主机是否存在因为管理不到位、信息摆渡没有严格按照相关规定执行等情况，而发生感染木马的安全隐患，并对高危的、已知或未知的木马及其危害进行定位和分析描述。



产品功能

1 静态分析

在木马的运行环境中通过木马的行为特征等发现可疑目标的技术。由于它不通过特征字的方式来进行检测，因此可以发现未知的疑似木马。但是由于系统无法智能的进行准确判断，可能还需要人工的经验来进行干预。包含下列功能项：

1) 隐藏进程检测　2) 隐藏端口检测　3) 内核模块检测　4) IE 检测
5) SSDT 检测　6) 自启动检测　7) LSP 检测　8) BHO 检测
9) DNS 检测　10) 隐藏服务检测　11) 文件关联
12) 系统账号　13) ini 配置文件检测

2 智能分析

通过特征字匹配的方式对已知木马进行检测，类似于现在的防病毒软件。此方法需要维护一个木马特征库，并不断对此特征库进行升级。如果与专业木马查杀厂商合作则会有更好的效果。此方法有优点是检查准确，比较明显的缺点是无法检测到未知木马和已知木马的变种而且检测速度比较慢。包含下列功能项：

1) 综合分析　2) 应用层木马分析
3) 内核木马分析　4) 进程综合分析

3 报表审计

生成检测报表及木马分析的结果报表，可选择报表的种类，自行输入检测的时间和地点，可存为.Doc 文件

产品优势

1 静态检测与动态检测相结合，确保检查效果

静态检测技术指的是通过特征字匹配的方式对已知木马进行检测，类似于现在的防病毒软件；动态检测指的是在木马的运行环境中通过木马的行为特征等发现可疑目标的技术。由于它不通过特征字的方式来进行检测，因此可以发现未知的疑似木马。两种技术相结合确保了检查效果明显有效。

2 底层技术应用，提高效率，降低用户空间开销

采用分级数据筛选与内存无关的组报技术，将海量信息有效缩减，并通过内核数据截取和预处理技术，大大降低了数据从内核空间拷贝到用户空间的开销，有效提高了系统工作效率。

关于鼎普

北京鼎普科技股份有限公司坐落于中关村软件园，是中国信息防泄漏的领航企业。鼎普科技创建于 2003 年，经过 8 年的快速成长，已成为国内信息防泄漏产品与解决方案的专业提供商，公司拥有 200 多人的专业团队，在全国各地拥有 5 家分公司和 7 个办事处，同时在北京、上海、成都、郑州、石家庄设立了五大客服中心，为众多的军队、军工企业、政府、高校、科研院所、金融系统和大型央企等客户提供及时、便利、真诚的服务。

鼎普科技拥有国际性标准水平的安全产品研发中心，中心设有信息安全攻防实验室、信息安全检查与评估实验室及新品研发等机构。在安全产品研发中心从事计算机、网络、电子信息应用等领域的顶级科技人才，通过长期对客户需求的理解与信息技术的研究，使鼎普科技的技术成为国内内网安全产品的标杆典范。专业从事信息安全的咨询顾问以其精湛的技术，帮助客户解决实际面临的安全问题，为客户呈现具有鼎普产品个性化、高效率的解决方案。

卓越的管理团队使鼎普科技通过了 ISO9001 质量体系认证、CMMI 三级认证、军工保密二级资格认证，获得了涉密信息系统集成资质、计算机信息系统集成资质，成为商业密码定点生产单位。取得了权威机构的各类资质认证 70 余项、专利 26 项。

作为“中国计算机学会计算机安全专业委员会”、“中国计算机学会信息保密专业委员会”和“全国信息安全标准化技术委员会”的成员企业，鼎普科技荣获了最具成长科技型 100 强企业、北京市专利试点企业、国家互联网应急服务支撑单位等多项国家级荣誉称号。为国防、国家奥运、神舟飞船等大型信息安全项目提供高品质的产品及服务，更获得了高度评价及认可。

鼎普科技旗下拥有信息防泄漏领域的领军品牌“鼎普”，同时拥有信息安全检查类第一品牌“猎隼”，秉承“更底层、更安全”的技术创新理念，与客户共同分享信息安全时代的无限精彩！