

特种木马防护坚固度检测及攻击演示系统

介绍 V1. 11

(文档编号：11301)



文档名称	特种木马防护坚固度检测及攻击演示系统		版本号：V1.11
拟 制	智华产品部	审 核：李中华	批准：郭子扬
发送组织		有效期：V1.12 版本发布前有效	
日期	2011 年 3 月 2 日	制作部门	产品部
修改类型	MODIFIED	修改部门	市场部

*修改类型分为 A - ADDED M - MODIFIED D – DELETE

特种木马防护坚固度检测及攻击演示系统介绍 V1.11

(Degree of protection of Ferry Trojan detection and demonstration system)

1. 引言

windows 操作系统的广泛使用和信息技术的迅猛发展，催生出了大量的计算机病毒和木马程序。其中以窃取秘密信息为目的的特种木马的出现，成为间谍木马技术发展的里程碑，其危害性已引起所有国家政府、军队等信息安全机构的高度重视。

北京智华天成科技有限公司联合中华人民共和国外交部，共同成立了国内第一个“摆渡型间谍木马攻防技术研究”科研小组，对摆渡木马的原理、特征、窃密过程进行了跟踪研究。目前，从全球安全机构的调查结果显示：摆渡木马已成为针对性和隐蔽性强、危害性大、特征变异快的间谍程序，是全球窃密效率高、窃密成本最低的间谍工具，也是当前计算机信息系统安全的最大威胁。

为了配合保密管理部门在检查、保密培训的过程中，形象而直观的演示摆渡木马的窃密效果，帮助党政机关单位的工作人员了解特种木马的攻击原理，目睹和感受特种木马的隐秘性和危害，警示各单位进一步完善计算机的安全防护措施。应各地保密局的要求，我们专门研发了一款具有安全控制的摆渡木马窃密软件——**特种木马防护坚固度检测及攻击演示系统**。

2. 系统概述

特种木马防护坚固度检测及攻击演示系统，是为了配合保密部门，检查各机关单位对摆渡木马防护是否有效，向各机关单位形象的演示摆渡木马的窃密过程和危害。

特种木马防护坚固度检测及攻击演示系统，可以作为保密部门检查内网防范是否有效的检查工具，以及保密部门培训、教学的一种辅助工具、保密部门在机关单位演示木马窃密活动的工具。

3. 系统特点和功能

1) 智能性

配置完全依照木马程序流程设计。配置功能强大，针对性极强，窃密过程隐蔽。系统的原理、特性、攻击流程完全按照特种木马原理设计，其内核技术性能强大、针对性

强，可以完全满足检测现有防护系统防护能力的需求。

2) 简便性

系统操作简单，无需任何特殊培训，会操作电脑即可使用。攻击演示过程形象直观展现特种木马窃密的全部过程。

3) 安全性

该系统本身具有很强的安全保护，不具有自我传播复制性，不具有系统驻留特征，在到达设定时间时自毁。主程序必须依托合法的安全钥匙才能运行，生成的检测和演示程序具有时效性，有效时间过后，所有功能会自动失效。同时，系统对配置的参数和窃取的文件信息进行详细记录。

4. 法律说明

特种木马防护坚固度检测及攻击演示系统，只能能用于保密局系统的针对特种木马防护坚固度的检测和现场演示，不得用于其它用途和目的。否则，产生的法律责任自行承担。

在网络安全的世界里，如果不想亡羊补牢，就要做到料敌之先！

北京智华天成科技有限公司

北京市海淀区紫竹院路 1 号人济山庄 C 栋 1905

电话: +86-10-51651800

网站: <http://www.waction.cn>