

安全周报

中国信息安全博士网

六月 第二期

二〇一〇年六月十二日

weekly.secdactor.com

- 学术会议
- 政府之声
- 病毒播报
- 产业动态
- 技术前沿
- 海外来风
- 黑客攻防
- 企业推荐



SMP-U

国迈移动存储设备管理系统

唯一三证齐全的移动存储设备管理系统

U盘系统核心功能：

- 杜绝U盘泄密事件
- U盘使用权限控制
- 防止U盘交叉使用
- U盘病毒主动防御
- U盘使用日志审计
- 适用于单机/网络

● 功能描述：

全国唯一三证齐全的U盘管理系统，通过国家保密局、解放军保密委、公安部三重权威认证。全网Internet告警中心+专用安全U盘+U盘管理系统“三合一”，对U盘、移动硬盘、手机存储、数码相机、MP3、MP4、各种CF/MD/SD卡/各类FlashDisk等移动存储介质进行分级注册，灵活控制U盘使用权限，防止信息泄密，记录使用日志，主动防御U盘病毒。杜绝因移动存储介质丢失、被盗用等造成的泄密事件。

■ Internet告警中心：

如涉密U盘违规外联到Internet，告警中心自动发出告警信息，并可查询到谁的U盘什么时间在哪台计算机（包括CPU、IP地址、MAC地址等）违规外联。

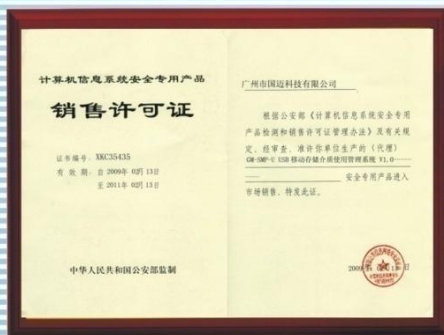
■ 专用安全U盘：

内部U盘、单向导入U盘、单向导出U盘、双向交换U盘。

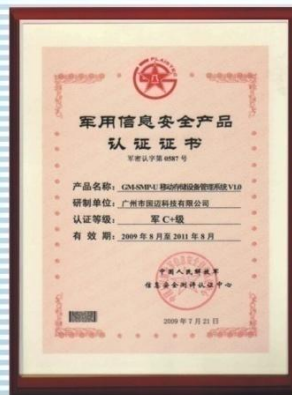
权威认证：



国家保密局认证证书
ISSTEC2008YT0618



公安部认证证书
XKC35435



解放军保密委认证证书
军密认字第0587号

成功案例：北京奥组委、解放军保密委、中国移动、中国边检、中国边防、某军工集团信息中心、总装某局、某卫星发射基地、中国兵器某研究所、中船舶某所、中国航天某设计院、某核辐射研究院、山东公安、广东公安、广东国安、河北检察院、广东省文化厅、洛阳有色金属设计院、机械工业四院、商丘电力、广东省第二人民医院、珠江医院、普利斯通、深圳电器、长丰集团、泰豪集团、汕头海关、北京大唐微电子、上海百联集团、深圳广前电力、河北建筑设计院、达尔嘉（亚洲）等。

防信息泄密，找国迈科技，要找就找最专业的！
更多信息，请登陆www.goldmsg.com

Guangzhou Goldmessage Technology Co., Ltd.



便携式计算机网络及 移动通信安全隐患展现系统

产品总述:

便携式计算机网络及移动通信安全隐患展现系统是一套能对网络信息系统和移动通信系统的多样化攻击手段、攻击方法、攻击后果、防护策略等进行直观展现的系统。

系统的成果包含当前主流的攻击方式和工具，展示各类网络隐患可能带来的攻击后果，便于系统管理人员、涉密人员及各级领导干部了解和学习各种攻击方式和防护方法，进而达到提高其忧患意识、责任意识和保密意识的目的。

便携式计算机网络及移动通信安全隐患展现系统的主要特性在于：全部采用便携式设备，方便携带，且配备投影仪，现场展示效果好。图形化操作界面、简明的操作手册，方便操作，实用性强。

展现的隐患种类较为齐全，功能丰富，更新速度快，新隐患出现后，会随时为用户进行升级和更新，并及时进行技术培训。

服务及时周到：为用户提供全面的技术支持与现场服务。

产品功能:

- 木马植入演示
- 网页篡改攻击演示
- U盘文件窃取演示
- 文件恢复窃取演示
- 网络钓鱼攻击演示
- 手机窃听演示
- 系统漏洞利用

国工信科技发展（北京）有限公司

地址：北京市中东路400号 邮编：102218 电话：8610-64126291 传真：8610-64126291
http://www.quogongxin.com email: secdoctor007@163.com



第三届中国信息安全博士论坛

(2010年7月31日-8月1日 宁夏·银川)



宁夏大学

欢迎您!

指导单位: 工业和信息化部信息安全协调司
教育部高教司
教育部高等学校信息安全类专业教学指导委员会

联合主办: 中国电子信息产业发展研究院
宁夏大学
北京电子科技学院

协办单位: 北京信息科技大学
北京交通大学
中国刑事警察学院

承办单位: 《信息安全与技术》杂志社
国工信科技发展(北京)有限公司

官方网站: 中国信息安全博士网 (www.secdactor.com)
第三届中国信息安全博士论坛官网 (meeting.secdactor.com)
教育部高等学校信息安全类专业教学指导委员会 (www.sec-edu.cn)

支持媒体: 中国电子报、中国计算机报、中国电脑教育报、通信产业报、中国经济和信息化、软件和信息服务、网管员世界、赛迪网、宁夏当地多家媒体

会议主题: 信息安全产、学、研的联盟创新与发展

会务组: 010-64126291 13661116129 张鹏飞

电子邮件: secdactor@163.com

会议官网: meeting.secdactor.com

目录

学术会议.....	7
2.0 时代的信息安全高峰论坛盛大召开.....	7
中国互联网软件行业自律圆桌论坛在京举行	8
2010 IBM 云计算高峰论坛 6 月 11 日在京召开.....	9
2010 年度 CIO 高峰论坛将于本月 30 日揭幕.....	9
政府之声.....	11
信息安全测评中心与微软继续安全合作	11
国新办发表《中国互联网状况》白皮书	12
中国反对任何形式网络黑客攻击行为.....	13
印度将就解决网络安全问题与电信商举行会谈.....	14
韩国政府网站遭攻击近 4 小时 疑与中国黑客有关.....	14
美 FBI 开始调查威胁信息安全的 iPad 漏洞.....	15
病毒播报.....	16
病毒监测周报 （2010.6.5-2010.6.11）	16
Mac 应用程序被发现含有恶意软件	17
Flash 曝重大安全漏洞 用户计算机或被黑客控制.....	18
假魔兽“台服”官网上线 包含恶意欺诈木马.....	18
“入侵者”变种 cl 和“卡徒杀”变种 hzt.....	19
黑客利用高考传木马 考生上网谨防毒	21
6 月第一周病毒报告 病毒少量下降	22
“简单百宝箱”遇“李鬼” 游戏玩家被盗号.....	24
产业动态.....	25
中国最大国家信息安全产业基地奠基.....	25
赛门铁克人为错误造成诺顿误删《魔兽世界》	25
谷歌发布云安全白皮书 拟提高安全问题透明度.....	26
美国最大云计算部署：微软击败 Google Apps.....	26
Twitter 遭遇技术问题 周二宕机 1 小时	27
Twitter 收购数据分析工具商 Smallthought	27
金山成立软件自律联盟对抗 360.....	28
技术前沿.....	29
电子政务系统中信息安全技术应用研究	29
网友发文揭穿 IPv9 奥秘 称域名转换类似 DNS 劫持	32
经济学家看云计算安全问题：发展是必然.....	33

颠覆传统 金山毒霸 2011 全面解决漏杀	34
IBM 高层首度回应“智慧地球”安全问题.....	35
黑客攻防.....	36
美网军司令：黑客每天刺探五角大楼网络 600 万次.....	36
网警教你识破八类网络骗局.....	37
69 圣战中韩黑客对攻 百度被黑无辜受害.....	38
安全预警：世界冰球迷成在线诈骗新目标.....	39
微软 6 月补丁修复 34 个漏洞 针对 Office 的攻击被缓解.....	40
海外来风.....	41
Visa improves security for online transactions	41
Google assures customers on cloud security practices	42
企业推荐.....	44
北京点聚信息技术有限公司	44

学术会议

2.0 时代的信息安全高峰论坛盛大召开

来源：中国信息安全博士网

6 月 10 日消息，今天在国家会议中心举办的“2010 年信息网络创新年会”上，举办了一个分论坛——2.0 时代的信息安全高峰论坛。论坛上，CISCO、JUNIPER、神州数码等十大公司就此次会议“明安全应用之道”和“优安全解决之术”探讨用户需求及应用热点以及全面解决方案及未来展望。



伴随互联网的飞速发展，中国网民数量迅速增长。据工信部最新数据显示，中国网民已达 4.04 亿，企业及各类机构的信息化应用突飞猛进，数据信息量呈裂变式爆发，由此引发的信息安全问题迫在眉睫。

那么，在 WEB2.0 时代信息安全最重要的解决任务或是重点又是什么。对此，国家信息产业部太极联合实验室主任、国信办专家、国家金卡工程办公室组组长、中国信息产业商会信息安全产业分会常务副理事长屈延文教授首先向大家讲到信息化科学，从信息化科学体系与计算机科学之间的差别来诠释信息科学的重要性；从脆弱性安全走向结构性安全引申到由于风险大、资本大等原因造成的金融危机；讲到传统科学、语言学，网络世界的行为学理论研究在中国，信息化研究是为了网络与生物，随后又提到中国研究网络世界计算机理论、中国研究新软件工程方法，并提出问题做出回答，屈延文教授诙谐的把行业协会企业比作“食草动物”，认为我们这些企业是在“信息化大草原”上翱翔打转，真正研究行为学的“食肉动物”屈指可数。最后，对未来的信息安全提出一些新的计划。之后，神州数码系统科技战略本部安全及系统管理本部技术总监刘毅提出了两点不同的见解。他认为信息安全最重要的是应用和数据的安全。有了数据即使一些架构丢失也可以利用这些数据重

新搭建。另一个就是，可不可以使用户从被动的防御变为主动地防御。用户投入了巨大的资金进行安全评估等等但是只是简单的打补丁修漏洞，而不是主动地管理我的安全。所以他认为应当使用户变被动为主动。

与我们一起关注 2.0 时代的信息安全高峰论坛，关注 IT 产业变革！

中国互联网软件行业自律圆桌论坛在京举行

来源：ZDNET 安全频道

6 月 10 日，中国互联网软件行业自律圆桌论坛在北京昆仑饭店举行，在论坛上，金山公司董事长求伯君表示，由于互联网化的进程，软件也在发生着诸多变化，但这也造成了一些同行间恶性竞争的出现，伤害到了用户利益，整合行业迫切需要厂商联合起来进行自律。

作为国内软件行业的元老级人物，求伯君在谈到初创阶段的国内软件业时表示，当时软件行业的气氛非常融洽，“我们当时一些比较早的人，像吴晓军，鲍岳桥这些软件行业比较早的人，还有严建东，王家民，我们的气氛都是特别友好，经常会在一起沟通，交流，气氛非常好，我们这一群人对软件是充满了热爱。我们今天仍然是对软件充满了热爱，我们大家提供的软件跟服务正在为中国三亿多电脑用户提供最优秀的服务。”

现在，软件的互联网化已经不可避免了，包括金山在内的很多传统软件都已经走在了互联网化的道路上。求伯君承认软件的互联网化为软件注入了很多新的活力，也为整个市场带来了生机，但他也表示“在互联网环境下，软件推广、运营、研发与过去有了很大的变化。在互联网时代，其实用户是很容易获得软件，升级也很方便，修改也很方便，同时我们也看到，互联网软件在电脑中的权利与作用越来越大，造成同行之间竞争越来越激烈，大家都想抢占用户电脑，这种情况下，我们作为互联网软件厂商应该更要反思，这个软件的权利到底有多大的底线？”

求伯君对于目前安全软件行业的频繁口水仗颇有微词，他表示口水仗是市场竞争变得无序的标志，在互联网环境中，很多软件厂商会急于推广自己的产品，因此造成了很多干扰用户的产品竞争格局出现。求伯君强烈抨击了这些行为，他表示做这样行为的软件从业人员“忘了作为软件人员最根本的出发点就是为用户服务。”他认为，如果软件行业的无序竞争持续下去，最终后果会造成对行业信任的集体崩溃。

为此，求伯君代表金山软件呼吁，中国的软件行业应该建立起良性的竞争环境，要做到切切实实的自律。具体而言，就是软件厂商之间要讨论怎么样建立一个让用户信任，对用户有益的良性发展的软件产业，并且能够落实到实处上，“让用户感觉金山的诚意，让用户选择我们的产品。”

在求伯君发言的最好，他表示对于中国软件行业还是充满着信心：“我始终相信，中国软件可以在互联网时代获得更快速的成长，中国软件产业也一定可以给用户带来最大的价值，认识自己的权

益，才可以让互联网推动整个世界的发展。”

随后，金山与其他九家软件与互联网企业共同发表了《互联网客户端软件自律宣言》。

2010 IBM 云计算高峰论坛 6 月 11 日在京召开

来源：比特网

随着计算技术的发展和商业的推动，云计算逐渐成为 IT 发展的趋势，并将带动 IT 产业的深刻变革，“不论你是不是愿意接受，云计算都正在改变世界”，作为最全面的云计算解决方案提供者、最富有经验的云计算解决方案实施者、最值得信赖的云计算解决方案合作伙伴，IBM 希望与您一起在转变中领先！

随着计算技术的发展和商业的推动，云计算逐渐成为 IT 发展的趋势，并将带动 IT 产业的深刻变革，“不论你是不是愿意接受，云计算都正在改变世界”，作为最全面的云计算解决方案提供者、最富有经验的云计算解决方案实施者、最值得信赖的云计算解决方案合作伙伴，IBM 希望与您一起在转变中领先！

6 月 11 日，携最新云计算智慧，“智揽云海 云领未来-2010 IBM 云计算高峰论坛”将在北京盛大召开，届时，IBM 智慧“云”集各方专家及客户，将在“构建智慧的地球”高度下从云计算的业务创新到实践应用，从战略远景到落地部署，系统全面地纵览云计算全貌。进一步帮助您深入把握云计算的实质内涵及发展趋势，斩获未来云计算发展先机。

战略高度：大会将全面梳理云计算，探讨现在与未来发展全貌；

中国特色：结合中国实际情况，全面解析中国云计算之路；

化云为雨：从解决方案到实践应用的全方位介绍让云计算变得触手可及

成功案例：分享 IBM 云计算方案在多个行业成功应用的案例，提供值得借鉴的实践经验；

自身分享：IBM 全球 CIO 届时将亲临现场，与您分享 IBM 利用云计算的实战经验

多角度探讨：大会将从业务、实施等角度，立体展示与讲解 IBM 云计算方案的独到之处。

互动演示：丰富全面的云计算解决方案演示，让您真实深入体验云计算

2010 年度 CIO 高峰论坛将于本月 30 日揭幕

来源：新浪科技

由工业和信息化部信息化推进司指导，《IT 经理世界》杂志社主办的，亚太地区最具影响力的年度 CIO 活动——“2010 中国 CIO 高峰论坛”将于 2010 年 6 月 30 日在海南三亚召开。

以“非常时期的 CIO 使命”为主题的“2010 中国 CIO 高峰论坛”，将重点探讨严峻的商业运行背景下，CIO 如何采用 IT 和互联网颠覆传统价值链，打通产业链上产品生产链和商品流通链的隔阂，帮助过剩的中国制造寻找新的出路；如何整合产业链资源，以价值网络的形态去应对严峻的商业环境，实现产业链的升级；如何在互联网上开拓新的价值空间，帮助企业寻找到新的市场；如何进一步挖掘企业的客户价值，拓展新的业务增长点；如何使精细化管理成为企业在非常时期必修的内功，用管理提升效率和利润空间。

在国际金融危机、中国经济结构调整和经济周期变迁三大外部环境背景下，如何保障中国企业业务连续性，如何加速中国企业转型升级，这不仅仅是企业家和 CEO 们的命题，也成为企业 CIO 们的命题。“2010 中国 CIO 高峰论坛”通过各界 CIO 的聚首和交流，旨在发现企业 CIO 制度建设对信息化建设的重要支持作用，并推动和促进企业信息化发展水平。本届论坛首次在工业和信息化部信息化推进司的指导下举办，同时也首次邀请美国、香港地区、台湾地区的 CIO 代表参加。

作为亚太地区规模最大，影响力最广泛的年度 CIO 专业盛会，中国 CIO 高峰论坛，自 2005 年开始定于每年年中举行，论坛主要邀请各行业顶级 CIO、知名学者、政府官员、知名跨国企业代表等齐聚海南三亚，共同探讨和分享企业信息化建设的经验与成果。

2010 中国 CIO 高峰论坛，将是 2009 中国优秀 CIO，中国重量级企业 CIO 聚首，信息化领域专家，重要企业代表深入探讨以上各种热点话题的盛会，将在这里发出 CIO 推动信息化变革的最强声音。

关于年度中国 CIO 论坛(CIO Forum)

从 2005 年开始，《IT 经理世界》每年在中国美丽的海滨城市三亚举办“中国 CIO 高峰论坛”，为中国顶级 CIO 提供了一个轻松开放、充分交流的机会。这是一个真正由 CIO 主导的论坛，CIO 自己设计话题、自己发言、自己组织讨论、自己担任主持人。五年来，共有近 1000 名来自各自领域的顶级 CIO、知名学者、政府相关领导和跨国公司专家参加论坛，共同体验这一绝无仅有的 CIO 盛会。中国 CIO 高峰论坛已经成为亚太地区规模最大，影响力最广泛的 CIO 专业盛会。

《IT 经理世界》是国内最早关注信息化及 CIO 成长的媒体，在 CIO 群体中有着重要的影响力。从 2002 年开始，《IT 经理世界》进行每年一度的“中国优秀 CIO 评选”活动，因其科学的评价标准、严谨扎实的工作作风以及众望所归的获奖者获得社会各界的一致赞同。通过评选，《IT 经理世界》与上千位的企业 CIO 建立起联系，与数百位 CIO 直接交流沟通，从 2002 年至 2009 年共有近 400 位优秀 CIO 获得奖项。从 2005 年开始，我们邀请获奖 CIO 和来自各行各业领域顶级 CIO、知名学者、政府官员和跨国公司代表在三亚举行高峰论坛，共同体验绝无仅有的 CIO 盛会——中国 CIO 高峰论坛(CIO FORUM)。

政府之声

信息安全测评中心与微软继续安全合作

来源: doit

日前, 中国信息安全测评中心正式与微软续签了新一期的政府安全计划源代码协议。该中心和相关被授权机构将被允许查看包括 Windows 7, Windows Server 2008 R2 在内的微软产品和平台源代码以及相关技术信息, 从而提高中国对微软产品安全方面的分析和测评能力。

本协议的签订和实施是国家发展改革委员会与微软公司 2006 年 4 月共同签署的关于加强软件产业合作备忘录(二期)的重要组成部分。国家发展改革委高技术产业司副巡视员徐建成、中国信息安全测评中心主任吴世忠和微软全球副总裁 Scott Charney 等出席了签字仪式。

政府安全计划源代码协议(GSP)是微软在全球的一个安全合作项目, 主要为政府机构及国际组织提供合法查看微软产品和平台源代码以及相关技术信息的途径, 从而增强对微软产品的安全性能方面的理解和信心。微软致力于满足政府和国际组织对于安全的特殊需要。政府安全计划源代码协议是其所做努力中非常重要的一部分。

2001 年, 微软推出了政府安全计划源代码协议, 旨在继续使 Windows 源代码对于其合作伙伴和客户更加透明。2002 年, 微软宣布可信赖计算计划(Trustworthy Computing), 将安全性置于微软开发所有产品的指导核心, 并且通过技术投资、客户指导和互动, 协作推动创建可信赖计算环境。政府安全计划源代码协议是微软可信赖计算计划的重要组成部分。

中国政府高度重视信息安全工作, 为了保障信息化进程的健康发展, 确保信息技术产品的安全可控, 专门成立了“中国信息安全测评中心”, 开展对信息技术产品和系统的安全性检测和风险评估工作。中国政府作为首批参加该计划的政府之一, 曾在 2003 年 2 月授权该中心与微软公司签署了第一期政府安全计划源代码协议, 获权查看当时主要相关微软产品的源代码和相关技术信息。经过几年的顺利合作, 随着微软产品的不断更新换代, 双方决定签署新一期的政府安全计划源代码协议。

根据签署的新协议, 中国信息安全测评中心和相关被授权机构将可以在线即时查看包括 Windows 7, Windows Vista、Windows XP、Windows Server 2008 R2, Windows Server 2003、Windows 2000 和 Windows 嵌入式 CE 6.0、5.0 版、4.2 版的专业版源代码包(“PSK”)以及 Microsoft Office 专业版 2003、Microsoft Office 系统中的任何附加产品等在内的微软产品的绝大部分现有版本源代码和相关技术信息。

除了能够查看源代码, 政府安全计划源代码协议还提供关于 Windows 平台技术信息的培训, 以增强政府建立和部署具备强有力的安全技术的计算基础架构的能力。

国家发展和改革委员会高技术产业司副巡视员徐建平表示: “全球范围内, 信息安全已日益成为一个

非常突出的问题，关系到国家的经济发展、社会稳定和公众利益，信息安全并不是某个国家或某个地区关注的问题，而是需要全世界共同面对和承担的一项艰巨任务。长期以来，中国政府高度重视信息安全。“十二五”期间，将进一步加强信息安全在信息化建设中的保障作用。政府安全计划源代码协议是国家发展改革委与微软公司关于加强软件产业合作谅解备忘录（二期）的重要组成部分，今天签字仪式的成功举行，表明双方的合作又向前迈出了积极的一步，希望微软公司与中国合作伙伴本着互利共赢的原则在信息安全领域进一步深化合作。”

代表中国政府与微软签署新一期协议的中国信息安全测评中心主任吴世忠说，“对信息技术产品的安全性实施测试和评估 是中国政府确保信息安全的重要手段之一。测评中心与美国微软公司在2003年签署政府安全计划源代码协议后，建立了相应的源代码查看与安全分析实验室，组织了一系列技术分析、培训和专家研讨。与微软公司的技术合作与交流，促进了我们对各类技术产品安全问题的分析研究，有效化解了相应的安全风险。过去几年的实践表明，双方建立的合作机制是有成效的，对更好的推进我国信息化的发展和维护我国的信息安全具有积极意义。今后，测评中心将继续利用 GSP 的合作机制，进一步促进与微软公司的技术交流，加深对微软产品安全性的了解和研究分析，不断提高有效控制安全风险的能力，在国家信息化建设中切实发挥好安全保障作用。”

微软全球副总裁 Scott Charney 表示：“实现可信赖的计算环境一直是微软努力的目标。我们很高兴与中国政府签署新一期的政府安全计划源代码协议。政府是我们的客户和相互信赖的合作伙伴，我们将向中国政府提供建立和部署安全计算环境的信息。”

微软大中华区董事长兼 CEO 梁念坚表示：“作为优秀的企业公民，微软扎根中国 20 年，一直积极与政府和行业等展开密切合作，致力于通过自身的技术优势帮助解决国家发展过程中的首要问题和社会需求，兑现‘同中国共同进步和发展’的承诺。新一期的协议是微软建立可信赖计算环境的重要努力之一，更是微软与中国政府长期密切合作的又一里程碑事件。”

国新办发表《中国互联网状况》白皮书

来源：新华网

互联网是人类智慧的结晶，20 世纪的重大科技发明，当代先进生产力的重要标志。互联网深刻影响着世界经济、政治、文化和社会的发展，促进了社会生产生活和信息传播的变革。

中国国务院新闻办公室 8 日发表了《中国互联网状况》白皮书。白皮书指出，中国政府充分认识到互联网对于加快国民经济发展、推动科学技术进步和加速社会服务信息化进程的不可替代作用，高度重视并积极促进互联网的发展与运用。

白皮书旨在介绍中国互联网发展的基本情况，说明中国政府关于互联网的基本政策以及对相关问题的基本观点，帮助公众和国际社会全面了解中国互联网发展与管理的真实状况。

白皮书分为前言、推进互联网发展与普及、促进互联网广泛应用、保障公民互联网言论自由、管理互联网的基本原则与实践、维护互联网安全、积极开展国际交流与合作、结束语等部分，全文约 13000 字。

白皮书说，中国政府把发展互联网作为推进国家信息化建设、实现经济社会科学发展、提高科技创新能力和人们生活质量的重要手段；积极营造有利于互联网发展的政策、法规和市场环境；通过完善国家信息网络基础设施、建设国家重点信息网络工程、鼓励相关科技研发、大力培养信息技术人才、培育多元化信息通信服务市场主体等举措，不断推动中国互联网持续健康快速发展，满足人们日益增长的信息消费需求。

白皮书指出，中国政府大力倡导和积极推动互联网在中国的发展和广泛应用。随着互联网在中国的快速发展与普及，人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化。目前中国已成为世界上互联网使用人口最多的国家。

白皮书说，建设好、利用好、管理好互联网，关系国家经济繁荣和发展，关系国家安全与社会和谐，关系国家主权、尊严和人民根本利益。积极利用、科学发展、依法管理、确保安全是中国政府的基本互联网政策。中国政府始终坚持依法管理互联网，致力于营造健康和谐的互联网环境，构建更加可信、更加有用、更加有益于经济社会发展的互联网。

白皮书表示，中国政府将不断完善互联网发展与管理政策，使其更加符合互联网发展与管理内在规律及客观需要。在实践中，中国政府十分注重借鉴各国发展与管理互联网的有益经验，并愿与世界各国一道共同促进世界互联网的繁荣发展。

中国反对任何形式网络黑客攻击行为

来源：新华网

中国国务院新闻办公室 8 日发布的《中国互联网状况》白皮书说，中国反对任何形式的网络黑客攻击行为。

白皮书指出，中国同世界其他国家一样，面临黑客攻击、网络病毒等违法犯罪活动的严重威胁。中国是世界上黑客攻击的主要受害国之一。据不完全统计，2009 年中国被境外控制的计算机 IP 地址达 100 多万个；被黑客篡改的网站达 4.2 万个；被“飞客”蠕虫网络病毒感染的计算机每月达 1800 万台，约占全球感染主机数量的 30%。

白皮书强调，中国法律禁止任何形式的网络黑客行为。《全国人民代表大会常务委员会关于维护互联网安全的决定》明确规定，对“故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害”等破坏网络安全的行为，构成犯罪的，依照刑法有关规定追究刑事责任。《中华人民共和国刑法》第二百八十五条、二百八十六条对非法获取计算机

信息系统中存储、处理或者传输的数据，对提供专门用于侵入、非法控制计算机信息系统的程序、工具等违法行为的刑事处罚作出了具体规定。

印度将就解决网络安全问题与电信商举行会谈

来源：新浪科技

印度政府周五表示，将在一周内与包括电信服务供应商在内的电信部门从业者举行会谈，帮助解决网络威胁问题。

印度电信业官员曾表示，今年早些时候，印度因安全顾虑，禁止国内的移动手机运营商购买中国华为和中兴通讯的电信设备。

印度担心来自中国的电信设备可能内置有间谍技术，会截取敏感谈话和政府文件，从而威胁其国家安全。

政府声明称，电信服务供应商应为他们的网络安全负责，印度政府将发布指导文件帮助运营商解决网络安全威胁。

韩国政府网站遭攻击近 4 小时 疑与中国黑客有关

来源：环球网

据韩联社 6 月 10 日报道，韩国行政安全部 10 日表示，韩国政府门户网站(<http://korea.go.kr>)9 日晚受到持续 220 分钟的分布式拒绝服务攻击(DDoS)，但因及时采取措施，未受损失。

韩国政府网站遭攻击近 4 小时



据韩国行政安全部称，攻击从 9 日晚 8 点 18 分开始，进行到午夜，共持续了 220 分钟。此次 DDoS 攻击来自 120 多个中国 IP，攻击开始 20~30 分钟后韩国行政部的政府电算中心切断 IP，有效抵

制了攻击。

目前，韩国行政部与国家情报院和广播通信委员会等相关机构分析攻击类型，追查攻击案犯，并密切关注国内外的网络攻击动向。此外，韩国行政部将此次事件通知给各道、市、郡的地方政府部门的网络管理人员和民间机构，要求加强戒备。

韩国媒体分析称，此次事件很可能与中国民间网络组织号召的“6.9 圣战”有关。“6.9 圣战”是指上海世博会期间出现哈韩族追星导致严重拥堵事件后，中国国内一些网络社区号召大家在 6 月 9 日这一天集中攻击 Super Junior 等韩流明星网站和贴吧的活动。

美 FBI 开始调查威胁信息安全的 iPad 漏洞

来源：天极网软件频道

据国外媒体报道，美国联邦调查局一名发言人表示，在苹果 iPad 曝出安全漏洞导致数万名用户的基本资料被泄露之后，美国联邦调查局已开始对其中潜在的信息安全威胁展开调查。

在信息被泄露的 11.4 万名 iPad 用户中，至少有一名是美国司法部工作人员。美国博客网站 Gawker 报道称，此次信息泄漏涉及的人士包括美国参议院、众议院、司法部、美国宇航局、国土安全局、联邦航空管理局和联邦通信委员会的人员。

美国司法部最知名的两名 iPad 用户为司法部长埃利克·霍德尔(Eric Holder)和国家安全顾问艾米·杰弗里斯(Amy Jeffress)。律师表示，iPad 在美国司法部内很受欢迎，因为这款平板电脑可以用于浏览 PDF 文档。

美国联邦调查局的调查并不仅限于美国政府工作人员使用 iPad 过程中面临的安全风险。而联邦调查局尚未就使用 iPad 向工作人员发出警告。

此次泄露的信息包括用户电子邮件地址，以及用于在 AT&T 网络中验证用户身份的 ICC-ID。不过安全专家表示，ICC-ID 泄露引起的安全问题很有限。

病毒播报

病毒监测周报（2010.6.5-2010.6.11）

来源：国家计算机病毒应急处理中心

国家计算机病毒应急处理中心通过互联网络监测发现，近期很多计算机用户受到“代理木马”新变种(Trojan_Agent.LY)的威胁。该变种集合了多种恶意程序软件的技术，采用了很多技术手段避开操作系统中防病毒软件的扫描查杀。变种还会在操作系统的应用程序接口处插入特定的指令代码，甚至对恶意程序代码采用多重加密等技术处理方式。

该变种运行后，会在系统的临时文件夹下释放病毒文件，修改注册表，实现其开机自动运行。迫使系统连接指定的服务器，在被感染计算机上下载其它病毒、木马等恶意程序。

另外，该变种具有分布式拒绝服务攻击的功能，即 DDOS 攻击。恶意攻击者可以通过控制大量受感染的计算机系统，向 Web 网站和计算机系统发送大量数据包，对其进行恶意攻击。同时，该变种还会修改受感染操作系统任务管理器中的自身程序进程名以便隐藏自己，使其很难被计算机用户发现。

目前，正值高等院校的毕业阶段，很多毕业生会通过互联网络中的招聘网站找到适合自己工作岗位。国家计算机病毒应急处理中心通过互联网络监测发现，恶意攻击者利用这个求职高峰期对这类招聘网站实施“网页挂马”，利用网页的高访问量，对浏览网页的求职者的计算机系统远程入侵访问，提醒这些求职者在浏览网页的同时，做好防护措施，防止自己的操作系统被入侵感染。

专家提醒：

针对上述新变种情况，我们建议广大计算机用户采用如下方法防范：

（一）针对已经感染该变种的计算机用户，我们建议立即升级系统中的防病毒软件，进行全面杀毒。

（二）针对未感染该变种的计算机用户，我们建议打开系统中防病毒软件的“系统监控”功能，从注册表、系统进程、内存、网络等多方面对各种操作进行主动防御，这样可以第一时间监控未知病毒的入侵活动，达到全方位保护计算机系统安全的目的。

Mac 应用程序被发现含有恶意软件

来源：TT 中国

防病毒厂商 Intego 的研究员警告说，一个新的恶意软件正在自由获取的屏幕保护程序中分布。称为 OSX/OpinionSpy 的间谍软件应用程序可以扫描文件，记录用户活动和发送窃取数据到远程服务器。

Intego 公司专门为苹果 Macintosh 电脑开发安全软件。该恶意软件并不新。曾在 Windows 机器上检测到其以前的版本。Intego 表示，根据它的行为，它被列为严重的安全威胁。

包含间谍软件的应用程序可以通过流行的下载网站来自由传播，包括 MacUpdate、VersionTracker 和 Softpedia。受害人不会注意到恶意软件正在下载，一旦恶意软件被下载到机器上，就很难检测间谍软件了。

Intego 公司博客发布警告说，“这些应用程序所提供的信息包含了误导性文本，即用户必须接受的解释是：‘市场研究’程序与它们一起安装。一些程序还直接从没有这些警告的开发商网站发布。”

安全专家指出，一个普遍的误解是：Macintosh 和基于 Linux 的机器比基于 Windows 的电脑安全。Windows 电脑经常被攻击者攻击，那是因为它们所占的市场份额很高；Mac 操作系统、基于 UNIX 和 Linux 的操作系统也包含可窃取敏感数据和执行其他恶意任务的漏洞。

苹果公司通过加入防病毒功能来回应，但对 Mac OS X Snow Leopard 来说还不是很成熟。苹果也将加入一些其他安全功能，如沙盒，以便从底层操作系统进程中隔离应用程序。除了 Intego，许多其他安全厂商包括赛门铁克和 McAfee 公司也出售 Mac 版的反病毒软件。

OSX/OpinionSpy 间谍软件可以打开一个后门，使恶意软件联系远程服务器来上载数据。该后门允许恶意软件自动更新新功能（在无用户干预的情况下）。

Intego 表示，目前还不清楚恶意软件复制并发送到服务器上的数据。恶意软件能够自动搜索本地网络数据包以收集数据。它扫描本地和网络容量，并可能获取用户名和密码、信用卡号码和其他敏感数据。该恶意软件还向用户浏览器和苹果的 iChat 应用程序注入代码。该行为类似于病毒。

Intego 说，“这种恶意软件在可以执行它的操作时，会‘感染’应用程序。它会感染 Mac 内存中应用程序的代码，但不会感染用户硬盘上的实际应用程序文件。

Intego 公司表示，它还发现了第二个基于 Mac 的间谍软件程序，并证明是一个 OSX/OpinionSpy 变种。

安全专家和 SANS 研究所讲师 Rob VandenBrink，在 SANS 互联网风暴中心日记中写道，恶意软件是一个简单的 bolt-on，可以很容易地添加到其他可自由下载的应用程序上。他说，该恶意软件是一个小型的 Java/PHP 应用程序，命名为 mac_flv_to_mp3.php。

VandenBrink 写道，“这一恶意软件可以通过大多数静态扫描测试——下载的软件本身是干净的，恶意软件是作为安装过程的一部分下载的。对 OSX 电脑用户来说，需要加强实时病毒扫描程序。”

Flash 曝重大安全漏洞 用户计算机或被黑客控制

来源于：搜狐 IT

据国外媒体报道，Adobe 在日前发布的重大软件安全公告中称，公司旗下 Flash Player 和 Adobe Reader 两款产品存在安全隐患，黑客可以利用该漏洞远程控制安装了上述软件的用户计算机。

受影响的软件包括：Adobe Flash Player 10.0.45.2, 9.0.262, 以及早期支持 Windows、Macintosh、Linux 和 Solaris 操作系统的 10.0.x 和 9.0.x 版本。

Adobe Reader 和 Acrobat 9.3.2 以及早期支持 Windows、Macintosh 和 UNIX 操作系统的 9.x 版本。

Adobe 公司表示，Flash Player 的 10.1 版本已确认不存在该缺陷，Adobe PDF 阅读器和 Acrobat 8.x 尚不能证实是否会受此安全缺陷的影响。

截至发稿时至，Adobe 尚未公布可以用以修复该漏洞的官方补丁。不过，用户可以通过临时删除 authplay.dll 文件或重命名等手段规避。(elite)

假魔兽“台服”官网上线 包含恶意欺诈木马

来源：ZDNet 安全频道

近日，金山毒霸云安全实验室检测到，多组以相近域名伪装为魔兽世界“台服”官网的欺诈网址上线，内含恶性欺诈木马。魔兽玩家在线搜索相关资料时，若未开启专业在线防护工具，和对网站域名未能加以识别，则会陷入黑客圈套，威胁到用户的财产安全。



假魔兽世界“台服”内包含恶意欺诈木马

据悉，当前很多玩家都在魔兽世界“台服”中在线游戏，对此，魔兽世界的“台服”官网 (<http://www.wowtaiwan.com.tw/>) 也成为了很多玩家查询资料和在线购买道具、装备的核心平台。更成为了黑客伪造欺诈网址，骗取用户点击而植入欺诈木马的关注焦点。如近日，金山毒霸云安全实验室，就检测到一组域名 (<http://www.wow-waigua.com>) 的欺诈网站。

此欺诈网站域名高度模仿魔兽世界“台服”官网，并通过搜索引擎的热词优化，使得用户在搜索“魔兽台服官网”、“魔兽台服”等信息时，极易不慎点击进入。网站实为假冒的大脚插件网站。它可能会欺骗您下载捆绑有病毒木马的游戏插件，甚至盗窃您的隐私数据等。



不慎点击欺诈网址，金山网盾可有效对其进行拦截

据金山毒霸反病毒专家介绍，类似伪装为所谓游戏“官网”的欺诈行为当前来看并不鲜见。从两组域名来看，相似程度也在九成以上。用户或在搜索过程中，或在通过IM软件、游戏聊天窗口中接收到对方发来的网址链接。一旦未能对齐加以识别和区分细微不同，便易落入黑客圈套。不慎访问钓鱼网址。

对此，反病毒专家提醒网友，“钓鱼”网站对于用户计算机会造成极大危害。用户在网上搜索或接受到相关链接时，应对网址内容加以细致识别，谨防部分域名高度近似的仿冒网址。同时，上网浏览过程中，开启金山网盾等专业在线防护工具，通过其对于各类恶意网址、钓鱼网站的有效识别，确保用户的在线搜索和浏览安全。

“入侵者”变种 cl 和“卡徒杀”变种 hzt

来源：eNet 硅谷动力

英文名称：Trojan/Invader.cl

中文名称：“入侵者”变种 cl

病毒长度：25876 字节

病毒类型：木马

危险级别：★

影响平台：Win 9X/ME/NT/2000/XP/2003/VISTA

MD5 校验：f6ac748bc1de8ce20208170c9cde0551

特征描述：Trojan/Invader.cl“入侵者”变种 cl 是“入侵者”家族中的最新成员之一，采用“Microsoft Visual C++ 6.0”编写，经过加壳保护处理。“入侵者”变种 cl 运行后，会在被感染系统的“%SystemRoot%\system\”和“%SystemRoot%\system32\dlldata\”文件夹下分别释放假冒的系统文件“dsound.dll”，还会在“%SystemRoot%\system32\”和“%SystemRoot%\system\”文件夹下分别释放“dsound.dll.dat”、“dsound.dll.LCEB”。在被感染系统的后台遍历当前正在运行的所有进程，一旦发现“360tray.exe”存在，“入侵者”变种 cl 便会尝试将其强行关闭，以此达到自我保护的目的。“入侵者”变种 cl 是一个专门盗取“legend of mir2”网络游戏会员账号的木马程序，其会在后台秘密监视系统中运行的所有应用程序的窗口标题。一旦发现指定游戏正在运行，便会利用键盘钩子、内存截取或封包截取等技术盗取网络游戏玩家的游戏账号、游戏密码、所在区服、角色等级、金钱数量、仓库密码等信息，并在后台将窃得的信息发送到骇客指定的远程站点上（地址加密存放），致使网络游戏玩家的游戏账号、装备、物品、金钱等丢失，给游戏玩家造成了不同程度的损失。

英文名称：Packed.Katusha.hzt

中文名称：“卡徒杀”变种 hzt

病毒长度：219648 字节

病毒类型：木马

危险级别：★

影响平台：Win 9X/ME/NT/2000/XP/2003

MD5 校验：12f6d3cec17cabf904f8054babad6760

特征描述：Packed.Katusha.hzt“卡徒杀”变种 hzt 是“卡徒杀”家族中的最新成员之一，采用高级语言编写，经过加壳保护处理。“卡徒杀”变种 hzt 运行后，会在被感染系统的“%USERPROFILE%\Local Settings\Application Data\”文件夹下释放恶意程序“837nU”、“ave.exe”、“GDIPFONTCACHEV1.DAT”。“卡徒杀”变种 hzt 运行时，会自动运行名为“xp security tool”的假冒安全软件。该软件会对系统进行病毒扫描，然后谎称在系统中发现病毒，并且诱骗用户购买该软件。其还会在被感染系统的后台连接骇客指定站点“76.76.*.219”，下载大量的恶意程序并自动调用运行。其所下载的恶意程序可能为网络游戏盗号木马、远程控制后门或恶意广告程序（流氓软件）等，从而给用户造成了不同程度的威胁。

针对以上病毒，江民反病毒中心建议广大电脑用户：

1、请将江民杀毒软件升级至最新版本，并且进行全盘扫描。江民杀毒软件增强了虚拟机脱壳与

启发式扫描技术，能够更加轻松地识别各种加壳、家族变种病毒，使病毒无所遁形。同时应用指纹加速、超线程扫描等高速扫描技术，更好更快地保护您的信息安全。

2、江民网络版的用户请及时升级控制中心和所有客户端，并且进行全网的病毒查杀，最大程度地保障企业的信息安全。

3、开启江民杀毒软件的主动防御功能。该功能采用智能沙盒技术，不仅可以更加准确地判别程序行为，还可迅速恢复病毒对系统造成的破坏与修改，令您轻松摆脱病毒的困扰。

4、江民杀毒软件拥有强大的自我保护功能，能够有效避免病毒的肆意破坏和干扰运行，为自身和系统同时加上了“金钟罩”般的强力保护。

5、开启江民杀毒软件的网页数据流监控功能。该功能可以更好地防御各种形式的网页病毒，为您的网上冲浪撑起保护伞。

6、开启江民杀毒软件的 BootScan 功能，在系统登陆前进行病毒查杀，清除顽固病毒更加方便、彻底。

7、建议使用安全专家内置的 RootKit 扫描功能。该功能可以对恶意程序深度隐藏的项目进行检测和清除，使恶意程序无处藏身。

8、建议使用安全专家内置的漏洞扫描功能。该功能扫描系统漏洞更加全面、准确，修复速度更加快捷。同时新增常见第三方软件漏洞扫描功能，使防护更全面，保护更彻底，不给病毒利用漏洞进行传播的机会。

黑客利用高考传木马 考生上网谨防毒

来源：eNet 硅谷动力

近日，金山毒霸云安全实验室截获了多组以“高考作文题目”、“高考录取查询”、“分数线查询”为名的欺诈网址，内含恶性网络木马，利用热点词汇进行传播，用户若未安装专业在线防护软件，极易遭受病毒威胁。

据金山毒霸云安全实验室统计数据显示，临近高考一周时间，针对高考相关的挂马、钓鱼网站一直处于上升趋势。因今年高考作文的题目今天刚刚公布，来势凶猛的挂马攻击或钓鱼攻击估计会在作文分数出来后变的更加有针对性。

每到高考，除应届考生外，高一、高二学生也格外关注今年的高考情况，“特别是今年的作文题目，”小范告诉记者，“所以今天中午时候我还特别网上搜索了下刚刚考完的作文题目是什么。”让小范意外的是，自己在点击一个 2010 高考作文讨论网站后，就出现了让电脑重启现象，重启后电脑也明显运行速度变慢了。

由此可见，如高考作文题目等，都成为了网民的关注热点，更成为了黑客的利用手段，作文题

目的新鲜出炉，对于关注今年高考、为明年高考做准备的高中生会通过网络查询，使恶意软件传播者不会轻易放过重大热门新闻事件

金山毒霸安全实验室反病毒专家提醒网民：网上搜索“高考饮食”、“高考作文”等相关信息时，应小心识别查询网站，避免误入挂马网站或者钓鱼网站。他表示，网页挂马从技术上已经完全可以实现很高的拦截率，网民只要安装金山网盾等专业防护工具就可以大大降低上网浏览网页时的中毒风险。若不小心中了钓鱼网站的陷阱，建议及时联系各地网警处置。

6 月第一周病毒报告 病毒少量下降

来源：比特网

本周总体病毒状况较为平静，未出现严重的病毒及网络安全事件。一周总的捕获样本数量较前周相比继续保持少量下降的趋势。

一周的常见病毒种类主要以网游盗号类/信息盗窃类木马程序(win32/gamepass 家族、Win32/wowpa 家族、Win32.Patchload 家族)、下载器类木马变体(Win32/silly 家族)、QQ 盗号类木马为主，新出现的变体数量本周也有所下降。

由于近期没有出现较易利用的新漏洞，因此近期黑客主要利用的漏洞相关的病毒变化不大，较常见的都是比较老的系统漏洞：

JS/CVE-2010-0249!exploit - IE 极光漏洞利用脚本

JS.MSDirectShowexploit - 利用 Directshow 漏洞；

JS.CVE-2009-1136exploit - Microsoft Office Web 组件控件中漏洞

HTML.Iframe!exploit - IE 脚本；

HTML.Emerleox.IJ - IE 漏洞相关脚本；

JS.CVE-2008-0015exploit - Microsoft Video ActiveX 漏洞

本周关注病毒：

病毒名称：Win32.Patchload.B

病毒别称：W32/Patched-DSound (McAfee), Virus:Win32/Patchload.A (Microsoft)

病毒属性：蠕虫

危害性：低危害

病毒特性：此家族病毒在近期的流行样本中较为常见。它们的部分变体具有感染可执行文件的行为。病毒对感染的文件做了入口点代码修改，当用户打开被感染的文件后，先执行病毒代码，再执行正常文件的代码。

感染方式：通过感染可执行文件传播。当用户执行病毒文件后，病毒程序将自身防止到系统可

行性文件后部，同时修改文件入口。执行病毒代码后切换到正常文件代码继续执行。在正常文件执行后，病毒线程同时被执行，线程执行后动态加载多个系统 DLL 文件，遍历%System32%目录下是否存在 arpcss.dll 文件，如有则退出线程，如没有则找到该文件并连接网络用于下载病毒文件并将下载的病毒文件保存到临时目录下。

危害：

连接网络下载其他病毒程序到本地目录，并在本机运行：

http://dydns175.3***.org:800/jax.exe

%System32%是一个可变路径。病毒通过查询操作系统来决定当前 System 文件夹的位置。

%Windir%

%DriveLetter%

%ProgramFiles%

%HomeDrive%

%Documents and Settings%

%Temp%

%System32%

本周常见病毒类表：

病毒名称	特性
GIF.Iframe!generic JPEG.IFrame!generic	在网页的图片尾部加入 js 脚本代码； 利用 IE 漏洞执行其中的脚本；
Win32.GameThief.F	近期最常见的木马程序也是数量最多的家族，本周共捕获 2 种变体；
Win32/Gamepass	近期最常见的木马程序也是数量最多的家族，本周共捕获 6 种变体；

Win32.Zuten!generic	盗取在线游戏的木马；
Win32.Wowpa	此家族属于记录按键的木马程序，它一般是被其它恶意软件安装。它尝试盗窃与 Massively Multiplayer Online Role Playing Game (MMORPG) "World of Warcraft"游戏相关的用户名和密码。
JS/CVE-2010-0249!exploit	IE 极光漏洞利用脚本
JS.CVE-2010-0806exploit	IE 漏洞利用脚本；
JS.MSDirectShowexploit	微软 DirectShow 漏洞类脚本，通常为挂马病毒使用。
Win32.QQPass	盗号木马类
Win32.Sality.AA	是一种多形态病毒，感染 Win32 PE 可运行程序
W Win32.VBDoor.BR	后门类程序，部分变体使用 MS-VB 编写
Win32.Lolyda.HK	网游盗号类木马
Win32.Patchload	下载器类蠕虫/木马；
Trojan.Win32.StartPage	修改 IE 等浏览器主页的木马程序；

“简单百宝箱”遇“李鬼” 游戏玩家被盜号

来源：eNet 硅谷动力

近日，可牛安全中心截获了一款“伪简单百宝箱”木马，该木马借仿冒简单百宝箱官网进行传播。木马一旦运行，就会进行窃取游戏账号等非法行为。安全专家建议，在百度中搜索“简单百宝箱”时，一定要认清官网地址，谨防冒牌官网木马；万一“中招”，可使用可牛免费杀毒进行查杀。

简单百宝箱是一款深受游戏玩家喜爱的游戏工具分享平台，但是近期有大量游戏玩家向可牛安全中心反映，在使用了“简单百宝箱”后，游戏账号被盗了。可牛安全专家分析发现，真正的简单百宝箱并未捆绑木马，游戏玩家是从仿冒网站下载了伪装的简单百宝箱。

山寨 “简单百宝箱”网站利用各种手段提高在百度中的排名

记者在百度中搜索“简单百宝箱”，发现出现了三个“官方网站”，经可牛安全专家鉴定，前两名均为病毒团伙制作的仿冒网站。安全专家表示，病毒团伙会利用各种黑帽 SEO 手段（甚至购买广告）提升仿冒网站在百度中的排名。在这些假冒网站中下载的“伪简单百宝箱”工具包含大量盗号木马。如果玩家不慎下载并运行了捆绑木马的伪简单百宝箱，就会遭遇游戏账号被盗的厄运。

据报道，国家互联网应急中心 2010 年一季度共收到 6225 个事件报告，这个数据与去年相比处于高位，其中网页挂马、网页仿冒事件的报告数量尤为突出。可牛安全专家提醒广大网民，上网冲浪时需开启可牛免费杀毒的实时保护功能，随时保护上网安全；并及时修复系统漏洞，定期进行病毒查杀，不给病毒木马可乘之机。

产业动态

中国最大国家信息安全产业基地奠基

来源：人民日报

天津国家信息安全工程技术研究中心暨产业化基地签约仪式 6 月 6 日在天津举行。国家信息安全工程技术研究中心、天津市科学技术委员会、天津市西青区委区政府和众多信息安全相关科研机构、信息安全领域专家及 30 多家入驻基地的国内知名信息安全企业参加仪式。

天津国家信息安全产业基地,是国家信息安全工程技术研究中心、天津市科学技术委员会和天津市西青区委、区政府共同支持建设的重大科技产业项目。基地坐落于天津市西青区学府示范工业园,总体规划面积 2600 亩,是中国最大的信息安全产业基地。该项目建设总投资 98 亿元。到 2015 年,产业基地将累计实现产值 600 亿元,引进和培育各类信息安全企业 150 家。

赛门铁克人为错误造成诺顿误删《魔兽世界》

来源：比特网(chinabyte)

据国外媒体报道,安全公司赛门铁克承认,最新的一次人为的错误造成诺顿互联网安全产品删除了流行的游戏《魔兽世界》的一部分内容。

赛门铁克产品经理 Kevin Haley 说,该公司的软件产品每个月会出现 10 至 40 次这种不正确的检测,也叫做误报。但是,大多数受影响的文件都不是广泛应用的。该公司副总裁级别的官员每个月都审查这些错误。

Haley 上周四在赛门铁克公司总部对新闻媒体说,我们对于《魔兽世界》出现的误报的情况。一位分析师查看了这个情况,他们做出了错误的判断。他们孤立地看待了这个问题。

Haley 说,更新版本的《魔兽世界》文件在分析计算机系统,从而使它看起来很可疑。赛门铁克通过自己的在线论坛获得了这个错误的通知,因此很快采取措施修复了这个更新。

他还说,杀毒引擎中内置的防御措施阻止了更多的严重的误报情况,如最近竞争对手 McAfee 删除一个关键的系统文件造成许多计算机不能启动。

赛门铁克称,即使发布了一个不正确的定义文件,赛门铁克的软件有一些安全机制阻止对系统文件造成破坏。

谷歌发布云安全白皮书 拟提高安全问题透明度

来源：互联网

谷歌想成为企业应用软件的龙头已经不再是个秘密。或许，有一天谷歌真的能够代替微软成为龙头老大。上周，谷歌全球销售运营和业务发展总裁 **Nikesh Arora** 在接受 **TechCrunch Disrupt** 采访时称，谷歌希望企业应用套件在未来三或四年内能给谷歌带来十几亿美元的收入。

谷歌应对云应用问题的挑战已经说服了企业。之前，一些应用程序用户质疑套件（包括电子邮件、日历、文档共享和聊天软件）的安全问题。为了使用户放心，使其安全措施、政策及涉及到谷歌应用程序套件的技术更透明，谷歌发布了一份白皮书。当然，白皮书还旨在向当前和潜在客户保证强大而广泛的安全基础。谷歌还创建了一个特殊门户，供使用应用程序的用户了解其隐私政策和安全问题。

这一白皮书概括了谷歌公司安全政策，包括信息安全、人身安全和运行安全。该文件似乎是为 IT 专业人士剖析准备的，因为非技术人员很少有人能明白这 14 页白皮书中阐述的大部分内容。

尽管现在谷歌可能在云应用问题上会面临一些审议，但云很可能是企业应用软件的未来。谷歌在云应用上下了很大赌注，甚至微软也在效仿谷歌。随着谷歌不断创新生产出面向企业的产品，如市场（**marketplace**）和企业应用引擎（**App Engine for businesses**），其业务重心将开始转移。而类似于白皮书之类的东西必将对谷歌业务过度有所帮助。

美国最大云计算部署：微软击败 Google Apps

来源：CNET 科技资讯

美国肯塔基州教育局通过微软证实，已部署微软的 **Live@edu** 服务，让该州逾 70 万名学生与教职员能使用这项服务。此举可望是目前为止美国境内最大规模的云计算部署行动。

这是微软迎战 **Google Apps** 战役获得的一大胜利，对微软提供的 **Live@edu** 服务来说也可能是重要的转折点。

这项从旧有 **Exchange 2003** 服务转换至云端访问的 **Exchange 2010** 迁移行动，也堪称是历年来最迅速完成的部署，估计只用一个周末的时间，就将 70 万个帐号迁移完毕。无疑地，是微软现有的技术，协助这场迁移行动顺利完成。

目前 **Live@edu** 的服务对象已扩及 1, 100 万人，遍布在全球 130 国、1 万所学校。

相形之下，**Google** 最近宣布，即时通讯工具 **Wave** 已对 **Google Apps for Education** 的使用者提供，并已发布迁移工具协助用户从 **Outlook** 转移至 **Gmail** 电邮服务。然而，这对 **Google** 使用者人数下滑的现象并未产生立即的影响；许多学生正移出 **Google** 在大学校园推出的测试服务。

其中一所学校是耶鲁大学，该校已停止 Google Apps 服务测试，微软宣称此举是该校对微软服务的背书。上个月，加州大学戴维斯分校以 Google 的“隐私保护水准令人无法接受”，表示计划停止测试 Google Apps。

Google 的 Apps for Education 网站宣称，目前在全球拥有 800 万名学生使用者，比微软目前服务的用户少了三分之一。虽然许多民间企业与组织偏好选用 Google Apps 来满足自家的协同作业需求，但学生市场在这方面还是难以把 Google 视为胜过微软的选项。

此举是否预示 Google 对学生提供的电邮服务气数已尽，或只是凸显 Google 应该更积极些，仍有待观察。

Twitter 遭遇技术问题 周二宕机 1 小时

来源：新浪科技

据国外媒体今日报道，Twitter 当地时间本周二早晨出现不明技术问题，网站和其应用程序接口(application programming interface, 简称 API)受到影响。该问题持续了近一个小时后被修复。

Twitter 在其官方博客 Twitter Status 上表示，尽管问题已经基本修复，但网站服务还未完全恢复正常。

“我们的系统于美国东部时间上午 11 点(北京时间周二晚 11 点)出现一个故障，导致 Twitter.com 在大约 1 个小时的时间内连续出现两次为期 30 分钟的宕机。”

网络监测公司 Pingdom 的数据显示，Twitter 6 月以来的表现相当稳定，只出现了一次 2 分钟的宕机。Twitter 5 月份发生总计 52 分钟的宕机，4 月份仅宕机 37 分钟。

随着 Twitter 在全球广泛流行，其稳定性开始备受关注。Twitter 今年 2 月表示，用户每天发表 5000 万条 tweet 信息，平均每秒发布 600 条。

Twitter 曾经因为其频频发生的宕机事件而臭名昭著，近来已有显著改善。去年 8 月，Twitter 发生超过 6 个小时的宕机事件，10 月又发生持续 5 个多小时的宕机。今年最严重的宕机发生在 1 月份，持续了 89 分钟。

Twitter 收购数据分析工具商 Smallthought

来源：搜狐 IT

北京时间 6 月 11 日消息，据国外媒体报道，微型博客 Twitter 当地时间周四宣布，该公司已经收购数据分析工具厂商 Smallthought Systems(以下简称“Smallthought”)。

Twitter 已经在内部使用 Smallthought 开发的 Dabble DB。Smallthought 新开发的 Trendly 能解析 Google Analytics 数据。

双方没有披露收购价格。

Twitter 高管凯文·韦尔(Kevin Weil)发表博客文章称,“Smallthought 员工已经加入我们的分析团队,致力于在我们当前的工具中整合 Trendly,为未来的广告客户合作伙伴开发创新性的实时数据分析工具。”

尽管 Twitter 商业模式的核心是“推广性 Twitter 消息”广告,但仍然希望为付费客户提供业务分析工具。Trendly 以及 Smallthought 的其他技术将有助于 Twitter 开发这类工具。

金山成立软件自律联盟对抗 360

来源: 新京报

金山安全和 360 公司之间的恩怨再次升级,昨天下午,金山联合百度、腾讯、卡巴、瑞星等 10 家公司成立软件自律联盟,而安全厂商中独缺 360。许久不曾在媒体公开露面的金山董事长求伯君昨天也出山助威。

金山认为 360 不够资格

求伯君在开场致辞中表示,“所有恶性竞争的最终后果都将导致用户对整个行业信任的崩溃,不管你是发起的一方还是被迫应战的一方。中国软件产业迫切需要一个可以良性竞争的环境,因此需要切切实实的自律。让用户选择相信中国软件产业。”

金山安全 CEO 王欣表示,360 之所以缺席,是因为“只有符合自律条件的企业才能加入联盟。”

昨天,求伯君正式回应“360 欲买金山毒霸”传闻。求伯君表示,从 1995 年微软开始想买金山到现在,已有不下 50 家企业想买金山,但金山想不想卖则是另外一回事。

360 斥资百万另立“联盟”

去年 7 月,360、金山曾同腾讯、百度等公司发起反网络病毒自律联盟,并共同签署《反网络病毒自律公约》,表示“遵守自律公约的条款,抵制网络病毒的传播、使用等不良行为。”

转过一年,金山牵头发起的软件自律联盟却独缺 360 一家。

而 360 也针尖对麦芒,在昨天上午宣传斥资 100 万元,资助“反流氓软件英雄”董海平成立“软件行为监督用户联盟”。

360 表示,该联盟将通过用户举报、网友评价、专家鉴定、定期公示等方式,推动互联网软件行业的行为规范,让网民能真正对自己的电脑“当家作主”。

360 公司总裁齐向东表示,“一些软件厂商利用网民不懂电脑技术的弱点,使得很多用户电脑‘被安装、被启动’了太多的软件。这些不规范行为,侵占了用户电脑硬盘、内存和 CPU 资源,导

致用户电脑性能急剧下降。”

金山股价遭重创

业内人士表示，求伯君近几年来很少在媒体上公开露面。此次出山应与金山安全和游戏两大业务均爆出不利消息，造成金山软件股价下跌有关。

5 月 25 日，360 公司董事长周鸿祎密集发布微博，披露 360 与金山的恩怨和杀毒行业互相攻击的黑幕，其中包括金山软件有漏洞等众多内容。随后，金山软件（03888.HK）股价在港交所两天内暴跌 13.88%，创下 52 周来新低，金山市值蒸发 6 亿港元。

另外，坊间传言“金山游戏 CEO 邹涛抛售个人所持金山股票，可能辞职”也成为金山软件股价下跌的助力。后来金山官方正式辟谣称绝无此事，表示在金山上市后，公司持有股票的高管及员工套现部分股票这些都是正常现象，邹涛减持也是正常资本行为。

技术前沿

电子政务系统中信息安全技术应用研究

来源：国脉金融服务网

应用信息安全技术提高电子政务系统的安全性是一个迫切需要解决的问题。本文首先剖析了电子政务系统信息安全方面存在的问题，其次研究了信息安全技术在电子政务系统中的应用，涉及到安全区域的有效划分、重要信息的有效控制以及系统 VPN 的合理设计等等，在一定程度上保证了电子政务系统的安全。

1. 引言

电子政务是提升一个国家或地区特别是城市综合竞争力的重要因素之一，电子政务系统中有众多的政府公文在流转，其中不乏重要情报，有的甚至涉及国家安全，这些信息通过网络传送时不能被窃听、泄密、篡改和伪造。如果电子政务网络安全得不到保障，电子政务的便利与效率便无从保证，对国家利益将带来严重威胁。因此，研究信息安全技术及其在电子政务系统中的应用具有重要的现实意义。

2. 电子政务系统信息安全存在的问题剖析

2.1 网络安全方面的问题

电子政务网在建网初期都是按照双网模式来进行规划与建设，即电子政务内网和外网，内网作为信息内部信息和公文传输平台，开通政府系统的一些日常业务，外网通过路由汇聚加防火墙过滤

接入主要向公众发布一些公共服务信息和政府互动平台。双网实现了物理隔离，建网初期往往只看重网络带来的便利与高效，但是并没有同步充分考虑安全问题，也没有对互联网平台的潜在安全威胁进行过全面综合的风险评估，网络安全建设严重滞后。网络安全方面的问题主要涉及到以下几个方面：

(1)来自内部的恶意攻击这种攻击往往带有恶作剧的形式，虽然不会给信息安全带来什么大的危害，但对本单位正常的业务数据和敏感数据还是会带来一定的威胁。

(2)移动存储介质的交叉使用，对于电子内网PC来讲，把上互联网的PC上使用过的U盘，移动硬盘都不能在政务内网上使用。U盘病毒和“摆渡”间谍木马会把内网中的保密信息和敏感数据带到互联网上，回传给木马的制作者。并且，这种病毒还会在内网上传播，消耗系统资源，降低平台的新能，影响政务内网各种业务的正常流转。

(3)内网的身份认证和权限管理问题。防止内网一般用户越权管理数据库，服务器，和高权限的数据平台。

(4)内网中使用的带存储芯片的打印复印设备离开现场返公司维修问题。

(5)政务内网中使用的各种损坏移动存储介质的管理销毁问题。

以上各个网络环节管理不好都会给信息安全带来潜在的隐患，会造成国家重要机密的泄密。

2. 2 信息安全管理方面的问题

有些政府单位存在只重技术，不重管理的现象，没有认识到人是信息安全的關鍵，管理正是把人和技术结合起来，充分发挥安全技术保障能力的纽带。总体上说，我国网络安全管理与保卫工作是滞后的。许多部门内部没有从管理制度、人员和技术上建立相应的安全防范机制，缺乏行之有效的安全检查保护措施。内部人员拥有系统的一定的访问权限，可以轻易地绕过许多访问控制机制不少网络维护使用人员缺乏必要的网络安全意识和知识，有的不遵守安全保密规定，将内网直接或间接地与因特网连接，有的安全设施设备的配置不合理，访问控制不够严格，这些问题的存在直接带来了安全隐患。

3. 电子政务系统中的信息安全技术的应用探讨

通常情况下，政务网建设将市、区县政务网连接在一起。为政府的内部办公和对外服务提供了极大的便利。本节针对以上提到的各种安全问题，探讨安全技术政务系统中的具体应用。

3.1 安全区域的有效划分

根据安全策略需要，安全域可以包括多级子域，相互关联的安全域也可以组成逻辑域。

电子政务网络域：网络基础设施层及其上层的安全保护功能的实现应由接入政务专网的用户系统负责实现。

电子政务业务处理域：电子政务业务处理域(简称“业务处理域”)包括那些在政务部门管理控制之下，用来承载电子政务业务系统的本地计算环境及其边界，以及电子政务信息系统的内部用户。业务处理域内主要包含相应政务部门的政务内网域、政务外网域和公众服务域，有些政务部门还有

内部自成体系的独立业务域。每个子域都对应的本地计算环境和边界。政务内网域与政务外网域物理隔离，政务外网域与公众服务域逻辑隔离。

电子政务基础服务域：电子政务基础服务域主要包括为电子政务系统提供服务的信息安全基础设施信息安全基础设施有：电子政务数字证书中心、信息安全测评中心、信息安全应急响应中心以及远程灾备中心等。

3. 2 重要信息的有效控制

电子政务系统的数据控制主要目的是阻止攻击者利用政务系统的管理主机作为跳板去攻击别的机器，但是只是尽量的减少，而不是杜绝这种行为。当然，针对政务内部网络任何的扫描、探测和连接管理主机是允许的，但是对从主机出去的扫描、探测、连接，网络安全系统却必须有条件的放行，如果发现出去的数据包有异常，那系统管理员必须加以制止。数据控制示意图如图 3—1 所示：

本文研究的政务系统的数据控制使用两层来进行数据控制：防火墙和信息检测系统(IDS)。

防火墙为了防止政务系统的管理主机被作为跳板攻击其它正常系统。我们必须对管理主机的外连接数进行控制，如只允许在一定的时一内发送一定数量的数据包。防火墙的主要功能是：设定单向地址拦截或双向地址拦截，在单向地址拦截时，一方到另一方的资料访问被禁止，但反向的数据访问依然能正常进行，不会受到影响；采用先进的状态监测数据包过滤技术，不仅仅是依靠单个的 IP 包来过滤，而是对每一个对话和连接进行分析和监控，在系统中自动维护其当前状态，根据连接的状态来对 IP 包进行高效快速安全过滤；对管理主机的外出连接进行控制。当外出连接达到一定数量时，阻断以后的连接，防止管理主机被攻击者攻破后用来作为发起攻击的“跳板对所有出入系统的连接进行日志记录。

3. 3 系统 VPN 的合理设计

使用 VPN，可以在电子政务系统所连接不同的政府部门之间建虚拟隧道，使得两个政务网之间的相互访问就像在一个专用网络中一样。使用 VPN，可以使政务网用户在外网就象在内网一样的访问政务专用网的资源。使用 VPN，也可以实现政务网内特殊管理的需要。VPN 的建立有三种方式：一种是 Internet 服务商(ISP)建设，对企业透明；第二种是政府部门自身建设，对 ISP 透明；第三种是 ISP 和政府部门共同建设。

在政务网的基础上建立 VPN，第二种方案比较合适，即政府部门自身建设，对 ISP 透明。因为政务网是地理范围在政务网内的计算机网络，它有运行于 Internet 的公网 IP 地址，有自己的路由设备，有自己的网络管理和维护机构，对政务网络有很强的自主管理权和技术支持。所以，在政务网基础上建立 VPN，完全可以不依赖于 ISP，政府部门自身进行建设。这样可以有更大的自主性，也可以节省经费。

3. 4 其他信息安全技术的使用

此外，电子政务系统的安全性可以采用如下的措施加以保证：控制对网络设备的 SNEP 和 telnet，在所有的骨干路由器上建立 accesslist 只对网管中心的地址段做 permit，即通过网管中心的主机

才能远程维护各骨干路由设备路由协议在不安全的端口上进行 Passive 防止不必要的路由泄露；将所有重要事件进行纪录通过日志输出：采用防火墙设备对政务局域网进行保护。

结语

总之，本文对基于互联网的电子政务系统存在的安全问题进行了深入的分析，在综合考虑成本和安全保障水平的基础上，运用信息安全技术，构建了一体化分防护安全保障体系。

网友发文揭穿 IPv9 奥秘 称域名转换类似 DNS 劫持

来源：IT 日报

几年前曾经打着维护中国网络主权的 IPv9 技术（或者被称为十进制网络）现在已经悄无声息，当初其发明人谢建平、十进制网络标准工作组及其学术团队一直以“商业机密”为由，拒绝公开有关 IPv9 的技术细节，不过最近一位名叫 yx9fun 的网友发文揭穿 IPv9 背后的奥秘。

数字域名类似 DNS 劫持

在当初的宣传中，IPv9 的最大特点是使用十进制数为网址编码，也就是说用户可以输入简单的数字域名如“12345”，来取代类似“www.abc.com”这样的域名。

yx9fun 详细解释了 IPv9 的实现过程。首先，从“十进制网络标准工作组”官网上下载一种插件，安装后，计算机系统中的注册表发生了变化，原本的 DNS 服务器（负责将域名解析成 IP 地址）被改成了一个陌生的地址——61.152.248.222，这其实是工作组提供的 DNS 服务器。如果你要登录的网站已经开始使用数字域名，比如“12345”，那么在浏览器中输入 http://12345 之后，电脑会连接到 61.152.248.222，用现有的 DNS 协议请求解析 12345，其实还是将 12345 解析为网站实际的 IP 地址，然后电脑根据这个 IP 地址再登录网站。

yx9fun 表示，整个过程跟常见的 DNS 劫持差不多，由 IPv9 直接修改用户 DNS 服务器地址，让用户在不知不觉中直接利用 IPv9 的 DNS 服务器进行解析。yx9fun 强调说，“这种做法类似以前 3721 的网络实名，在地址栏输入中文名字的时候，就能打开所对应的网站，同样是需要安装插件才能实现。”

IPv9 地址只是计算游戏

事实上，所谓的 IPv9 地址根本不需要向“十进制网络标准工作组”申请，它实际上只是一个简单的计算过程。现在普遍采用的 IP 地址（IPv4 地址），本身就是 4 位的 256 进制数。比如 64.233.189.104 是 Google 的 IP 地址，用“ $104+256\times 189+256\times 256\times 233+256\times 256\times 256\times 64$ ”相加的方法可以得到一个数字 1089060200，安装插件后，直接在浏览器中输入 http://1089060200，就可以打开 Google。

按照 yx9fun 的提示，记者对 IT 时报网站的 IP 地址也进行了测试，根据公式换算后，得到了 3729045999 这个“IPv9 地址”，在安装了官方网站所提供的插件后，直接在浏览器中输入 <http://3729045999> 后，便正常打开了本报网站的首页。

最终目的是谋利

如同前面提到的，IT 时报的 IPv9 地址 3729045999 并不容易记忆，如果要拿到一个更容易记忆的、类似 1234567 的 IPv9 数字域名，就必须向十进制网络（中国）信息中心（IPv9 的具体运营企业）申请付费才行。

在“十进制网络标准工作组”官网上，记者找到了一份“DNIC 地址分配联盟费用说明”的文件，该文中提到了一些付费原则：“新申请成为联盟成员的单位，需交纳 2 万元的开户费；联盟成员 IPv9 单次申请地址量按 8000 元每 17 个地址收取，不足 17 按 17 计算；联盟成员按 DNIC 分配的 AS 号码（也就是所谓的靓号）数量交纳 AS 号码年费：按 10000 元/年每个 AS 号码收取。”等等。

yx9fun 对此提出了自己的看法，“十进制网络标准工作组”的本质是做类似“QQ 靓号”的生意，卖十进制的域名，然后谋利。

经济学家看云计算安全问题：发展是必然

来源：全球 IP 联盟

安全在一定程度上阻碍了云计算的发展。在现今的商业环境中，由于数据和信息至关重要，所以企业对数据非安全性因素非常恐惧。思科董事长兼 CEO 约翰·钱伯斯曾在公开场合表示，云计算是大势所趋，但却会对网络安全技术产生极大影响，我们应当对云计算的普及欢欣鼓舞，因为这会推动我们设备的销售。但这又是一场安全恶梦，而且无法通过传统方式解决。

尽管客户可以通过云计算享受外包服务，也可以租用现成的系统来处理自己的数据和业务，并且这么做的成本远远低于传统方式。但客户更担心安全问题。

虽然目前的技术解决方案可以降低安全风险，但所有的 CIO 们仍旧感到不安，而解决这一问题的唯一有效的“方法”就是“等待时间”！因为企业完全接受云计算这个概念，并且放心地把自己的数据及应用程序托管到自己不能掌握的地方，的确是一个复杂的过程。

经济学家在看待这一问题时非常有趣，他们这样说：

云计算的发展与经济的发展相当类似。人类的文明开始于贸易，而最初人们只是以物换物，而后来人类发明了硬币，这使贸易变得更便捷，但人们仍旧不得不随身携带沉重的“财富”。纸币的出现是经济虚拟化的第一步。后来出现了期票、债券，它们本来没有价值，而国家迫使人们认可这个概念，并证明这是一个真实的东西。后来就产生了金融工具，如股票。股票、债券这种共同基金的出现创造了分享财富的方式。当一个人不使用这些财富时，其它人就可以用。这和云计算分享资源

的方式如出一辙！

这的确有些神奇！有趣的是，云计算的使用率对于中小企业和大型企业来说没有区别。云计算以其强大的灵活性与伸缩性吸引了所有人的目光。随着时间的推移，人们将更习惯于用工具和虚拟的网络来掌握和处理信息，正如人们用写在纸上的数字代表自己的财富！

从这样的角度来看，云计算的安全问题并不能阻碍它的长远发展。云计算代表的是一种更先进的思维方式，它的发展是一种必然，所以它是 ICT 技术发展的未来！

颠覆传统 金山毒霸 2011 全面解决漏杀

来源：赛迪网

你的电脑里有漏杀病毒吗？金山毒霸安全实验室最新研究报告显示，每年被各种杀毒软件“漏杀”掉的病毒木马多达 100 万个之多，近三成中国网民电脑中存在漏杀病毒。产生“漏杀”问题的根本原因是什么呢？杀毒软件又将如何规避解决“漏杀”问题呢？金山毒霸云安全实验室反病毒专家建议广大用户，解决漏杀问题，必须选择新一代的、真正的云安全杀毒软件。

传统杀软“技术软肋”导致漏杀必然存在

分析漏杀产生的根源，是传统杀毒软件的识别方法无法适应计算机病毒木马的快速增长，需要从识别方法上进行根本的革新。

传统的病毒识别方法是检测黑文件，而黑文件的数量却是日新增数万种，厂商永远没有能力收集完所有的病毒文件。这一点，从各厂商每年公布的病毒统计报告就可以看出，没有任何两个厂商收集的病毒数量完全一致。

云杀软，全面解决“漏杀”问题

基于对漏杀问题分析和研究，金山安全实验室得出结论，只有应用型技术的专业“云安全”杀毒软件，才能全面解决用户说面临的“漏杀”病毒现象。

作为国内首款真正的云杀毒软件，金山毒霸 2011 采用的“可信云安全”技术，是目前中国互联网最大的云安全体系，可以 100% 鉴定用户电脑上的正常文件。同时，强大的自动分析鉴定体系使互联网上 95% 的新未知文件，在 60 秒内即返回鉴定结果，应用精确样本收集技术更使文件鉴定准确率达到了 99% 以上！以此为基础，只要不是正常的文件，就可以当作对用户有安全威胁的程序进行隔离。从而实现了“检漏”的目的。

1. 查杀能力更强，让病毒无处可逃

病毒木马数量增长迅速，2009 年有 2000 万种之多。那是否有必要每次做安全扫描都把所有应用程序全部和数千万乃至上亿种病毒特征完整检查一遍？下次杀毒，再重复这个过程呢。金山毒霸认为，传统杀毒理念已经进入死胡同，照传统思路做杀毒软件将会让用户的电脑变得越来越慢，电

脑运行也会越来越没效率。

在金山毒霸 2011 中，只需将流行最广、危害最严重的病毒特征库缓存到本地。同时，将绝大多数用户能遇到的正常文件白名单库也缓存到本地，其它海量文件特征库放在云端。这样一来，金山毒霸 2011 的查杀率得到了全面提升，也在一定程度上解决了漏杀问题。

2. 响应速度更快，最大限度缩短漏杀期

金山云安全服务端采用了超过 20 种鉴定方法，包括虚拟机、启发式分析、沙盒技术、动态行为分析、API 序列分析等等，新的分析方法还在不断改进和增加中。多种分析方法并行、相互纠错，能在 1 分钟内完成 95% 的文件鉴定。这些鉴定方法对病毒作者来说，是完全不可见的，他们无法知道金山是用何种手段在对付病毒木马，也就无法拿出针对性的绕过或反制手段，因此金山毒霸 2011 的漏杀几率就很小。

此外，金山毒霸 2011 是目前市面上唯一一款设计了兼容模式的杀毒软件，当你的电脑已经安装其它杀毒软件时，再安装金山毒霸 2011，会自动启用兼容模式。在这种工作模式，金山毒霸 2011 会成为病毒扫描器，防御会自动关闭，不会出现程序冲突。并且，处于兼容模式运行的金山毒霸不会拖慢系统速度。

因此，即使你的电脑中已经安装了其他杀毒软件，依然可以安装一款金山毒霸 2011，使用金山毒霸 2011 检测一下电脑中是否有漏杀的病毒木马，让自己的电脑更安全。

IBM 高层首度回应“智慧地球”安全问题

来源：互联网

针对《第一财经日报》报道的《工信部重估 IBM “智慧的地球”战略安全性》一事，IBM 高层和 IBM 官方首度作出回应。IBM 大中华区董事长及首席执行官钱大群昨天告诉本报，IBM 正在和国内很多研究单位研究如何解决好这个问题，这是一个大的课题，会有很多不同的解决方案，“关键是如何帮助国内完成转型的问题。”IBM 官方也向本报记者提供了一份针对“智慧的地球”安全性的声明：“对于安全问题的关注是合理的。”

IBM 认为，“智慧的地球”的举措，不会损害国家安全和信息安全，“也不会影响政府对于关键信息的控制。”它能够带来的，是对数据更好的使用（以我们的客户所决定的方式），让数据更加具有意义，并帮助预见业务运营的结果。

此前，本报曾经报道政府部门和研究机构正在对“智慧的地球”战略安全性一事进行评估，而有关“智慧地球”、物联网安全的数份报告，已送至国家有关方面，并得到高度关注。

IBM “智慧的地球”计划是未来十年中 IBM 战略发展的核心，IBM 每年的研发投入达 60 亿美元，其中一半都用在“智慧的地球”项目上。

“智慧的地球”战略被提上桌面是在 2009 年 1 月 28 日。当天，美国工商业领袖举行了一次圆桌会议，IBM CEO 彭明盛向美国总统奥巴马抛出这一概念。该战略定义大致为：将感应器嵌入和装备到电网、铁路、建筑、大坝、油气管道等各种现实物体中，形成物物相联，然后通过超级计算机和云计算将其整合，实现社会与物理世界融合。在此基础上，人类可以更加精细和动态的方式管理生产和生活，达到“智慧”状态，提高资源利用率和生产力水平，改善人与自然间的关系。

随后，“智慧的地球”在奥巴马的推动下上升为美国国家战略。而中国对物联网的发展也高度重视，并将此称为传感网。

昨日，IBM 咨询服务部门宣布和金蝶达成战略合作，将在原有资本合作的基础上，开展更多的业务合作，包括各自成立专门的团队，向中国客户提供“金蝶软件+IBM 服务”，并根据中国市场特点，帮助金蝶向服务型公司战略转型，同时推进 IBM “智慧的地球”在中国市场的布局。

黑客攻防

美网军司令：黑客每天刺探五角大楼网络 600 万次

来源：中国新闻网

据新加坡“联合早报网”报道，美国网军司令亚历山大指出，五角大楼网络每天遭到黑客刺探(Probe)次数多达 600 万；他担心美国电脑系统受到“远程敌人”的攻击会增加。

据报道，美国网军司令部最近才刚正式成立，主管是四星上将亚历山大(Keith Alexander)。亚历山大也是国家安全局局长。他担任网络司令后，在美国战略与国际问题研究中心首次发表的公开演讲中表示，他上任后的首要任务是，研发美国军事网络遭受威胁的实时图景；并着手制定对此威胁进行反击的条规。

亚历山大指出，五角大楼系统每小时遭到 25 万次外来探测，一天下来就多达 600 万次。

亚历山大说，美国“国防部需要维护 700 多万台机器的安全，和这些机器连接的网络有 1.5 万个。”

他说，美国网军司令部的工作是“阻止、侦查、防御美国电子空间面临的威胁”。他认为美国的国家利益受到威胁，这是因为来自国外的行动者、恐怖分子、犯罪集团、个别黑客的阵容越来越强大，以致美国“非常容易遭到攻击”。

亚历山大指出，组成国家和军力的每个环节能否有效运作，电子空间是个关键，国家数据必须受到保护。

他说，从蛛丝马迹判断，一些来自远方的入侵者瞄准某些系统准备进行破坏，今天要搞这种破坏和毁灭是有可能做到的，也是美国必须认真对待的。

他希望军方和政府提高监控电脑网络实时状况的能力。他指出美国的网络形势警觉性非常有限，对整个网络系统也没勾勒出共同行动的路径图。

他指出，在面对网络攻击时，要如何应对，这都需制定出“明确的交战规则”。

俄罗斯曾向美国提出建议，签订一份限制网络战条约。亚历山大认为，俄罗斯的建议“可以作为国际讨论的起点，”但他说，讨论的级别应当是“比我更高”。

亚历山大还认为，网络安全须涉及私人部门的合作。

他说，维护网络安全不仅是军方的责任，同时也是全国性的安全课题，应动用各种工具和全国的力量加以解决。

网警教你识破八类网络骗局

来源：互联网

近期网络诈骗案件高发，（重庆）市公安局发布警情提示：当心购物诈骗等八类网络骗局。

针对八类主要网络骗局，昨日，市公安局向广大市民支招：上网时要做好电脑安全防范工作，及时下载更新防病毒软件，开启相关安全保护功能；不要下载来历不明的软件，防止个人资料信息被盗取和利用。

警方同时称，市民要积极了解各类网络诈骗手法的特点，提高安全防范意识：对于亲友或合作伙伴在网上发出的汇款请求不要轻信，一定要以电话或其他方式进行核实；对于网上出售的商品价格明显低于市场售价的应留个心眼，尽量选择收到实物后再支付的付款方式，不要轻易汇款；对于网上发布的中奖信息、彩票预测信息和股票投资信息切不可相信，犯罪分子正是利用“天上掉馅饼”的侥幸心理设置圈套；网上慈善捐款或使用网上银行、网络交易平台进行汇款支付的，应仔细核对网址是否正确；对于网上发布招聘信息要求先付会员费、中介费的不可轻信，应去正规的求职网站咨询。

这八类网络骗局你碰到过吗

1 冒充亲友诈骗

采用欺骗或黑客手段获取受害人亲友 QQ 号等网上联络方式，然后冒充受害人亲友借钱，更有甚者，播放受害人亲友的视频聊天录像，以达到取信受害人目的。

2 冒充商业伙伴

通过欺骗或黑客手段获取了受害人商业伙伴的电子邮箱后，利用该电子邮箱或注册用户名为相似的邮箱名，冒充其商业伙伴对受害人实施诈骗。

3 网上购物诈骗

在互联网交易平台开办网店，或直接开设购物网站，以明显低于市场的价格在网上兜售数码产品、游戏装备、监控器材等商品，诱使网民与其联系购买。

4 虚构中奖诈骗

通过电子邮件、QQ、论坛短信、网络游戏等方式发送中奖信息，诱骗网民访问其开设的虚假中奖网站，再以支付个人所得税、保证金等名义骗取网民钱财。

5 彩票预测诈骗

不法分子开设彩票预测网站，以有内幕消息、权威预测等为名，大肆吹嘘其历史预测成绩，诱骗网民汇款加入成为其会员。

6 股票预测诈骗

不法分子开设股票投资网站，冒充正规证券公司，以有内幕消息、权威分析等为名，大肆吹嘘其历史投资成绩，诱骗网民打款进行投资。

7 钓鱼网站诈骗

开设网址与真实网站极为相似的虚假网上银行、虚假慈善网站或虚假网络交易平台，骗取网民身份信息、银行卡信息和密码，从而盗取网民银行存款。

8 网上招聘诈骗

不法分子在各大网站、论坛上大量发布虚假的招聘信息，引诱网民在网上应聘，再以收取“会员费”、“介绍费”等名义骗取网民钱财。

69 圣战中韩黑客对攻 百度被黑无辜受害

来源：eNet 硅谷动力

6 月 10 日消息 昨天凌晨 1 点左右，硅谷动力资讯中心获悉，因为 69 圣战，中韩黑客双方在互联网上“对攻”，而百度则首当其冲成为了黑客大战受害者。

据一知情人士向硅谷动力资讯中心透露，昨晚 1 点左右，百度首页呈无法访问状态，在几分钟内刷新后，仍显示“域名无法解析”，该网友的截图中显示了百度被黑时无法打开的页面。

不过，另有说法称，百度首页是在 1:30 左右被黑客篡改，其链接指向了 Google。

一位网友向硅谷动力资讯中心讲述了百度被黑的过程。“我在凌晨 1:30 分左右访问百度时，竟发现百度的搜索按钮”百度一下“变成了”Google 一下“。页面刷新后还是老样子。”该网友表示，“在过了大约有 5 分钟左右，访问百度时，则被转到另一个百度的域名”www1.baidu.com“，这个网站就没了刚才那种情况，又过了 5 分钟再访问百度，就一切恢复到从前了！”

据悉，百度被黑客攻击很可能起源于 69 圣战事件。在该“圣战”中，中韩双方黑客向对方国家

的网站发起了攻击，部分韩国网站被中方黑客挂上了“红旗”，而中国方面，百度则成为了韩方攻击的对象，首页被“黑”掉数分钟。

什么是 69 圣战

所谓“69 圣战”是指韩国明星团体 SuperJunior 在世博会演出时本来预定发票数千张，但最终只发票 500 张，从而造成大批粉丝在场外造成混乱、踩踏，甚至在混乱中有粉丝向阻止进入场馆的志愿者和武警吐口水。随后，以“魔兽世界吧”为发源地，在天涯、猫扑等网站出现了网友组织的反对 SuperJunior 及粉丝的活动，众多网民相约相约在 6 月 9 日（昨天）7 时在知名论坛和网站对韩国明星团体及粉丝进行爆吧。

安全预警：世界冰球迷成在线诈骗新目标

来源：赛迪网

即将在南非展开的 2010 年世界杯足球赛，是现今体育史上受到最高度瞩目的赛事。如同预期一般，网络犯罪份子们也已利用这个赛事，来做为他们成串永无止息诈骗营利的另一个手法。

TrendLabsSM 的工程师们发现两款不同的垃圾讯息皆利用了此赛事活动。第一封垃圾邮件附加了一个 .DOC 档案附件，向收件者声称是由国际足球协会组织委员会协办的新抽奖竞赛的最后通知。并告知收件者奖金为美金 55 万元。不过如果要领取此笔奖金，“赢家”必须立刻和邮件中所指定的代理商联络。该封邮件同时要求收件者提供个人数据。

和此诈骗相关的另一个样本是一封撰写得相当差劲的电子邮件，并附有一式文字同样拙劣的 PDF 信件附件。这一封要求收件者透露特定资料以汇转一笔金额高达 1 千零 50 万美金的款项。如同意此提议，收件者将可获得该笔金额的 30%。

这个手法利用的是声名狼藉的 419 奈及利亚诈骗手法(419 or Nigerian scam)，该手法利用承诺支付巨额款项给合作者的方式，来说服使用者先行付费。

典型的奈及利亚诈骗案 (Nigerian Scam) 是诈骗类型的一种，受害者被承诺只要能提供数据或透过垃圾讯息(见图 3)支付一小笔捐款费用，即可获支付一笔如乐透奖金，遗产继承等之金额。信件一开始(1)介绍据称是来自某知名机构的寄件者。接着恳求收件者的协助。我们所取得的世界杯足球赛主题的垃圾邮件(见图 4)就使用了同样的手法，即(2)承诺支付收件者一笔金额。

这两起诈骗皆未直接索求金钱。相反的是，他们要求的是数据或是要使用者(3)与一家假公司配合，(4)将他们的联络数据传送给该公司。简单的说，这些诈骗后幕后的网络犯罪份子皆是恶意使用者，利用因特网来进行如身份窃盗，散发垃圾讯息，网络钓鱼，及其它类型诈骗等的犯罪活动。事实上，国际足球协会(FIFA)在以下的部落格贴文中，以类似的在线诈骗内容等严正警告球迷：

2010 FIFA World Cup Spam Strikes Again(2010 年世界杯足球赛垃圾邮件再度出击)

Scammers Attempt to Score Through the FIFA World Cup(诈骗者企图利用世界杯足球赛赢利)

微软 6 月补丁修复 34 个漏洞 针对 Office 的攻击被缓解

来源: <http://netsecurity.51cto.com>

微软月度安全更新连发 10 个安全补丁, 用来修复 Windows 操作系统以及 IE、Office 等软件中的 34 个安全漏洞。值得关注的是, 办公族常用的 Office 软件一下暴露出 10 多个漏洞, 即便是装了 Mac 版 Excel 的苹果电脑, 同样需要打好补丁。

根据微软的官方公告显示, 此次发布的 10 款补丁中, 有 3 款补丁程序的安全级别为“严重”, 属于威胁程度最高的级别, 其中 2 个用于修复包括 Windows7 在内的操作系统漏洞, 另 1 个用于修复 IE 浏览器漏洞。其余 7 款补丁程序的安全级别则为“重要”, 仅次于“严重”级别, 这些补丁主要用于修复包括 Mac 版 Excel2004、2008 在内的 Office 和 Sharepoint 等安全漏洞。

尽管外界普遍认为 Windows7 和 IE8 采用了更好的安全机制, 甚至被奉为防范挂马网页的“黄金搭档”, 但随着用户基数增加, 在大批黑客的潜心挖掘下, Windows7 和 IE8 被发现的安全漏洞也与日俱增, 仍然需要安全软件的全面防护。此外, Office 也是漏洞不断的重灾区, Office xp、2003、2007 无一幸免, 而且大多为远程代码执行漏洞。即使是苹果电脑用户, 如果装了 Mac 版 Excel, 也得及时打好补丁, 否则极易在不知不觉间就受到黑客的“遥控”攻击, 使重要的办公资料被木马窃取。

据 360 安全专家介绍, 微软 6 月补丁不仅数量多, 而且涉及到系统内核和 Office。从以往网民打补丁的问题反馈来看, 这两类补丁安装失败、造成系统和软件故障的概率较高, 特别是在各种第三方美化版、Ghost 系统上, 还可能出现蓝屏、Office 打不开等现象。为此, 360 安全卫士 7.1 版漏洞修复模块进行了优化升级, 不仅会提示用户一键自动修复漏洞, 还能根据电脑系统环境智能选择该打的补丁, 并独家提供经过 360 测试调整的补丁安装包, 最大程度帮用户打好补丁。

海外来风

Visa improves security for online transactions

Source: www.infosecurity-magazine.com

Visa has launched a payment card in Europe to improve security for online transactions.

The CodeSure card contains a keypad and an eight-character display for showing a one-time passcode for any Visa debit or credit card.

"As the cardholder is required to enter their Pin [personal identification number] for every online transaction, the CodeSure card will prevent any unauthorised use", Visa said.

The company has taken the step because online transactions are more susceptible to fraud as they do not use the Pin.

Online transactions often rely on information printed on the card and hackers who have these details may be able to make a purchase online.

Visa's Verified by Visa and MasterCard's SecureCode systems provide additional security, but still rely on a static password, which is vulnerable to hacker attacks.

The CodeSure card overcomes that vulnerability by displaying a unique one-time passcode after users enter their Pin using the keypad on the card.

"This is an extremely convenient way to bring a similar level of security to payments online as we now enjoy on the high street with chip and Pin", said Sandra Alzetta, head of innovation at Visa Europe.

The CodeSure card goes beyond online banking and shopping and also allows organisations to use the card in place of other online log-in systems to access, for example, corporate virtual private networks, she said.

Visa 增强在线交易安全

来源: www.infosecurity-magazine.com

——中国信息安全博士网

visa 在欧洲已经推出安全码认证卡，以提高网上交易的安全性。

该卡包含一个键盘和一个用于显示一次性密码的借记卡或者信用卡的八个字符的显示屏组成。

“每一次网上交易要求持卡人必须输入密码（个人识别号码），安全码认证卡将防止任何未经授权的人使用”，Visa 说。

该公司已经采取了措施，因为网上交易更容易受到欺诈，并且发现网上交易一般不使用个人识

别号码。

网上交易往往依靠卡里的信息，黑客拥有了这些资料就可以进行在线购买。

通过 visa 的验证和 MasterCard 的安全码认证卡提供额外的安全性，但这仍然依赖于一个静态密码，很容易受到黑客的攻击。

安全码认证卡通过展示一个独特的一次性密码，克服用户使用键盘输入卡密码的脆弱性。

“这是一个非常方便的方法来实现类似网上付款这样的安全水平，正如我们现在喜欢在大街上刷卡及密码并用一样，”桑德拉阿尔泽塔，Visa 欧洲区创新部门负责人说。

“安全码认证卡不仅用于网上银行和购物，而且也允许企业使用该系统在其他的地方登录访问。例如，公司的虚拟专用网，”她说。

Google assures customers on cloud security practices

Source: Computer weekly

Google has issued a white paper on the security of its Google Apps service to assure existing and potential customers about the security of its cloud-based services.

The white paper includes information about Google's security practices, policies and technology that support Google Apps, and attempts to counter the perception that Google's online services are less secure than traditional on-premises systems.

Yale University in the US halted its move to Google's Gmail and Google Apps in March, citing security and privacy concerns.

But Eran Feigenbaum, director of security at Google's enterprise group, said in a blog post that the move is part of Google's move towards increased transparency.

"We are always improving and evolving the security of our systems, and we work every day to help protect against new threats", he wrote.

Feigenbaum highlighted some of the key points in the white paper:

Google datacentres are protected by advanced physical security controls, and access to information is monitored at multiple levels.

Google stores customer data in fragments across multiple servers and across multiple datacentres to both enhance reliability and provide greater security than can be achieved by storing all data on a single server.

Google performs software patching rapidly across identical server stacks to help keep users updated with the latest patches.

Administrators can set fine-grained access controls for documents, calendars, and other types of information commonly stored in the cloud.

Operations at a vast scale can help detect security threats across the web early and prepare appropriate defences.

System redundancy involves data replication across disparate datacentres for availability and disaster recovery.

谷歌云安全保证客户的做法

来源：计算机周刊

——中国信息安全博士网翻译

谷歌已经发布了应用服务安全的白皮书，以确保有关基于云安全服务的现有客户和潜在客户的安全。

白皮书包括谷歌的安全实践、政策和技术的信息，并且试图证明谷歌的在线服务比传统在线服务系统安全的多。

美国耶鲁大学在 3 月处于对安全和保密的考虑，停止了其邮件系统和应用系统，向谷歌邮箱和应用系统转移。

但是谷歌企业集团的安全主任 Eran Feigenbaum，在博客里说“这种转移是谷歌转向增加透明度的一部分”。

他写道，“我们总是改进和完善我们系统的安全，并且我们每天去抵抗新的威胁”。

Feigenbaum 指出了白皮书的关键：

谷歌数据中心受先进的物理安全控制器的保护，以及对信息的访问会受到多层次的监控。谷歌在多个服务器上存储的客户数据并且数据跨多个数据中心，以加强双方提供信息的可靠性和安全性，这样比所有数据存储在一台服务器上安全的多。

谷歌服务器在执行相同的软件补丁时是非常快的，以保持客户能够得到及时的更新。

管理员可以通过限制条件对数据库中的文件，日期，和其他类型进行设置。

通过巨大的规模的操作可以帮助我们在早期发觉网络上的安全威胁，以及做适当的防御准备。

数据冗余是通过在不同数据库之间复制而产生的，它表现为两方面一个是数据的可用性另一个是数据恢复的灾难性。

企业推荐

北京点聚信息技术有限公司

点聚信息技术有限公司是一家以计算机软件开发和服务为主营的公司。公司始终本着技术为本，服务为先的精神，坚持不懈的致力于中间件，应用程序的研究和开发，在电子政务，文档处理，办公自动化等方面为各企事业单位和个人提供了优秀的软件产品和服务。

点聚在不断发展的过程中，逐步形成了众多具有自主知识产权的软件产品。目前已有多家非常有实力的软件企业与点聚达成了战略合作关系，例如汉王、吉大正元、八大国家和省级 CA 等，均在自有系统里集成了点聚签章产品，最终用户近千家，包括人民银行、工商银行、中国联通、国家档案馆、人民日报社、三大军区、二总部、中国核工业集团、中国国电集团、中国人寿、阳光保险、安邦保险、首钢集团、宝钢集团等大型企事业单位。点聚出众的技术实力、服务能力和良好的信誉赢得了用户的广泛称赞。

AIP 版式：全方位领先国内其它产品，转化质量、速度，浏览速度，独有的证书加密授权机制，多级安全控制，是我们最高端的一款电子签章产品。

PDF 签章：盖章时无需安装 Acrobat 专业版，浏览和验证时只需安装免费的 Acrobat Reader 即可实现。

Office 签章：我们提供雾化功能，防拷屏防复制，如防止通过写字板打开、截屏、数码相机拍摄等方式非法复制印章图片。在文档锁定状态下，提供含数字签名的文字批阅功能，满足逐级批阅需求。支持各种骑缝章方式。

含数字签名二维条码打印防伪，能校验纸质页面内容是否被篡改。

支持手机移动签章，支持 Windows Mobile 和 Windows CE 系统

“沟通，务实，创新，奉献”是我们点聚人在公司发展过程中所形成的自身特质。

点聚公司将积极的和各界朋友紧密合作。一如既往的致力于中国软件产业的快速发展，为中国软件产业的振兴做出我们不懈努力。

浪潮SSR成为

" 中华人民共和国第十一届运动会唯一指定服务器操作系统安全加固系统产品 "



浪潮 主机安全的领导厂商

浪潮SSR (Server System Reinforcement) 服务器安全加固系统是基于对信息安全等级保护制度及相关标准的深入理解,以构建安全的计算环境为基础,以强制访问控制为主线,结合当前信息安全产业的发展现状而推出的专门针对服务器操作系统的整体安全解决方案。SSR采用先进的ROST技术理论,在操作系统内核层对服务器操作系统进行加固,同时根据信息安全管理中的“三权分立”原则,实现对用户和进程的最小授权,防止对系统文件和重要数据的误操作,从根本上免疫目前针对操作系统的各类攻击行为,彻底防范病毒、蠕虫、黑客攻击等对操作系统和数据库的破坏。这一独到的服务器系统安全解决方案填补了国内在此领域的长期空白,浪潮信息安全被赞誉为“服务器安全专家”,开辟了信息安全产业发展的新方向。

浪潮SSR产品系列

SSR企业版:企业核心主机操作系统免遭受非法攻击的“智能屏障”

SSR网络版:可信服务器安全运维中心

SSR专用版:为您的主机系统量身订做的“安全胃甲”

主要功能

从根本上免疫针对服务器操作系统的攻击
符合国家信息安全等级化保护三级标准
有效防止内、外网针对服务器系统的攻击
保障业务的连续性、稳定性、安全性及可靠性
有效解决了安全体系中系统层的安全问题
从根本上防范冲击波、震荡波等蠕虫类病毒



inspur 浪潮

中华人民共和国第十一届运动会
IT产品与服务合作伙伴

浪潮信息安全事业部

北京办事处:北京市海淀区阜成路73号裕惠大厦1002室 邮编:100142

电话:010-68451517 (总机) 传真:68451517-6688

成都办事处:成都市一环路南一段22号红瓦大厦930 邮编:610041

电话:028-85243518 传真:028-85214223

杭州办事处:杭州文三路478号华星时代广场A楼1507 邮编:310012

电话:0571-88907770 传真:0571-88907772

南京办事处:南京市中山北路45号华美达怡华酒店7层 邮编:210008

传真:025-83308166

安徽办事处:合肥市长江中路436号金城大厦1301室 邮编:230061

广州办事处:广州市天河区河北路898号信源大厦17层 邮编:510698

电话:020-38182808-8208 传真:020-38182825

上海办事处:延安西路129号华侨大厦23楼 邮编:200050

传真:021-62485588-9075

太原办事处:太原市平阳路东巷56号7号楼5单元201室 邮编:030012

济南总部:济南市山大路224号1号楼1层东厅 邮编:250013

技术支持热线:0531-85105399 0531-88932888 (总机) 转5399

售后服务热线:0531-85105398 0531-88932888 (总机) 转5398

E-mail: Security@inspur.com