

安全周报

第三期

二〇一〇年四月十六日

weekly.secdotor.com

中国信息安全博士网

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



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

广州办事处：广州市天河区北路898号信源大厦17层 邮编：510898

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

目录

政府之声.....	4
李毅中：推手机网络实名制保网络信息安全.....	4
《通信网络安全防护管理办法》公布.....	6
学术会议.....	7
第九届中国互联网大会将于 8 月在京举行.....	7
高端容错计算机发展战略论坛在京召开.....	10
产业动态.....	11
Options Media 集团借道网秦进入手机安全市场.....	11
蓝港王峰：王江民时代是技术天才大草莽时代.....	12
江民科技后继有人 王江民之子接手管理.....	14
惠普成功收购 3Com 公司.....	16
VB100 测试赛：国际大厂失手 中国杀软表现良好.....	18
正日益扩大的外包安全服务业.....	21
布鲁科特发布业界首个 IPv6 Web 安全网关.....	23
瑞星杀软网络版新品正式发布.....	24
ERM 为勘察设计企业知识产权保驾护航.....	27
金山成立安全子公司称将全面互联网化.....	29
瑞星“打黑”：力推云安全.....	30
假冒杀毒软件增长 占恶意在线广告的 50%.....	34
病毒播报.....	35
本周病毒预报（4.12—4.18）.....	35
技术前沿.....	36
曲成义：信息安全的理解和全局对策.....	36
云的安全和云安全.....	38
威胁隔离！用 SELinux 保护虚拟化.....	41
云计算与网格计算 基于网络的不同技术.....	46
四步预防恶意软件威胁.....	50
探析网络安全与防范技术.....	54
黑客攻防.....	58
微软下周发布 11 个安全补丁 修复 25 处漏洞.....	58
Sun Java 漏洞影响 Java SE 6 到 10 版本.....	58
Facebook 农场被指含嵌恶意广告 导向假冒网站.....	60
QQ 申诉系统疑存在严重漏洞.....	62
Java 漏洞致 Windows 面临攻击危机.....	63
自学成才网络高手攻击金盾网.....	65
黑客利用 Java Web Start 安全漏洞展开攻击.....	65

政府之声

李毅中：推手机网络实名制保网络信息安全

文章来源：通信产业网

4 月 13 日消息，近日，工业和信息化部部长李毅中出席 2010 年经贸形势报告会，并作“当前我国工业发展的若干重大问题”的专题报告。李毅中在报告中谈到了关于要高度重视网络信息安全的问题。李毅中指出，目前，世界大多数国家的手机、网络都采用实名制，但在我国还缺乏法律依据。要借鉴国外的先进管理经验，推行手机、网络实名制，加强备案审核。

李毅中表示，目前，信息产业加速更新换代已经成为国际大趋势，软件服务的网络化、开源化深入开展，集成电路、数字视听、半导体照明等电子技术正在催生着新的经济增长点。但网络的信息安全问题必须高度重视，决不能掉以轻心。

信息产业面临更新换代

“信息产业面临更新换代迅猛发展的新形势，发展是第一要务。”李毅中分析指出，信息技术在驱动了上一轮技术革命以后，势头始终不减，宽带、无线、智能等网络技术加速更新换代，计算机的处理速度已经达到 1000 万亿次/秒，云计算、量子计算、光子计算等技术加速发展，极有可能推动信息产业实现新的质的飞跃。同时还会带动互

联网、电子商务、文化创意等多个产业强劲增长,创造新的商业模式。

李毅中在报告中指出, 我们必须牢牢把握发展的机遇, 加快实施“核高基”等重大科技专项, 突破一批核心技术, 带动集成电路设计制造、关键领域软硬件研制生产、电子元器件品质升级;加快推进三网融合, 推动宽带无线通信、下一代互联网、数字化广播电视网的发展;做好高端网络设备的研发和产业化, 加快推进传感网研制, 实现下一代互联网从 IPV4 向 IPV6 的过渡, 实现与通信网、互联网的结 合, 推动传感网的商业化。

借鉴国外经验 推网络手机实名制

在针对手机、网络实名制问题上, 李毅中表示, “我们高度重视网络信息安全, 采取了一系列措施。我们作为互联网的行业主管部门, 目前正在积极参与开展为期一年的打击手机淫秽色情专项行动。本着标本兼治、重在治本的原则, 我们正在研究逐步实施手机、网络实名制。”

李毅中强调指出, 目前, 世界大多数国家的手机、网络都采用实名制, 但在我国还缺乏法律依据。要借鉴国外的先进管理经验, 修订《手机信息管理办法》和《互联网信息服务管理办法》, 推行手机、网络实名制, 加强备案审核。同时, 要加快研究对网络域名和 IP 地址管理的有效办法。”

此前, 在 2 月 21 日, 工信部在京召开干部大会上, 李毅中作了主题为《当前经济形势的几个热点问题》的经济形势报告。李毅中在

报告中指出，当前，网络信息安全面临严峻挑战，保障安全是第一责任。李毅中表示，“网络安全要标本兼治，重在治本，目前相关部门正研究实施手机、网络实名制。” 3 月 5 日，在全国两会上，李毅中在回答记者关于网络实名制的提问时表示，网络实名制是个大方向。

《通信网络安全防护管理办法》公布

文章来源：中国通信运维网

根据工信部令，《通信网络安全防护管理办法》已经 2009 年 12 月 29 日中华人民共和国工业和信息化部第 8 次部务会议审议通过，现予公布，自 2010 年 3 月 1 日起施行。

根据《通信网络安全防护管理办法》，通信网络安全防护工作坚持积极防御、综合防范、分级保护的原则。制定这个办法的目的，是为了加强对通信网络安全的管理，提高通信网络安全防护能力，保障通信网络安全畅通。办法明确，中华人民共和国境内的电信业务经营者和互联网域名服务提供者管理和运行的公用通信网和互联网的网络安全防护工作，适用该办法。

工业和信息化部负责全国通信网络安全防护工作的统一指导、协调和检查，组织建立健全通信网络安全防护体系，制定通信行业相关标准。各省、自治区、直辖市通信管理局依据该办法的规定，对本行政区域内的通信网络安全防护工作进行指导、协调和检查。

办法明确, 通信网络运行单位应当按照电信管理机构的规定和通信行业标准开展通信网络安全防护工作, 对本单位通信网络安全负责。通信网络运行单位新建、改建、扩建通信网络工程项目, 应当同步建设通信网络安全保障设施, 并与主体工程同时进行验收和投入运行。通信网络安全保障设施的新建、改建、扩建费用, 应当纳入本单位建设项目概算。

办法要求, 电信管理机构应当对通信网络运行单位开展通信网络安全防护工作的情况进行检查。这些检查包括: 查阅通信网络运行单位的符合性评测报告和风险评估报告; 查阅通信网络运行单位有关网络安全防护的文档和工作记录; 向通信网络运行单位工作人员询问了解有关情况; 查验通信网络运行单位的有关设施; 对通信网络进行技术性分析和测试; 法律、行政法规规定的其他检查措施等。

办法还明确, 对于违反该办法有关条款的, 由电信管理机构依据职权责令改正; 拒不改正的, 给予警告, 并处五千元以上三万元以下的罚款。电信管理机构的工作人员违反有关条款的, 依法给予行政处分; 构成犯罪的, 依法追究刑事责任。

学术会议

第九届中国互联网大会将于 8 月在京举行

文章来源 中国物联网

4 月 7 日上午，由中国互联网协会主办的 2010（第九届）中国互联网大会暨第二届中国网民文化节新闻发布会在京启动。会上宣布，2010 中国互联网大会（www.2010cic.cn）将于 8 月 17 日至 8 月 19 日在北京国际会议中心隆重举行，本次大会将主题定为：“服务——网络价值之本；绿色——网络发展之道”，倡导注重责任、促进和谐，打造更融合和可持续发展的互联网。大会将延续“一会一节一盛典”理念，与第二届中国网民文化节深度融合，呈现一届更具人气、更富创新、更有活力、更见实效的行业盛会。发布会上，第二届中国网民文化节（www.wangminjie.cn）同步启动。2010 中国互联网大会中英文官方网站（www.2010cic.cn）也于今日全球同步上线。

中国互联网协会秘书长助理石现升主持发布会。

工业和信息化部电信管理局业务资源处王安平出席发布会并致辞。王安平提出：在后金融危机时代，作为中国经济增长动力之一的中国互联网行业，应积极寻求产业发展的新途径、新思路、新服务和新潜质，为整个社会注入更多经济增长的新动力。王安平表示：工业和信息化部将一如既往地支持中国互联网协会工作，支持中国互联网大会，并希望在全行业的通力协作下，创造出一届诚信、创新、繁荣的互联网行业盛会。

中国互联网协会副理事长高新民发表主题演讲，详细阐述了 2010 中国互联网大会的主题含义。高理事长指出，如何更好地利用和创新互联网的服务、挖掘网络的巨大潜力和价值是本届大会着力探讨的要

点。中国互联网协会将继续发挥行业组织优势，通过行业自律等方式号召业界共同努力，为互联网行业健康、繁荣发展贡献力量。

中国互联网协会业务拓展部孙永革部长以及中国互联网大会组委会副秘书长曾明发分别介绍了 2010 中国互联网大会总体情况、特色亮点及第二届中国网民文化节精彩互动活动内容。2010 中国互联网大会除继续强势推出已有的品牌论坛外，还将针对世界 500 强企业的 IT 信息服务实践、网络文化产业、网络媒体、“宅经济”等热点新增多个特色论坛。较之往届，今年大会将更加注重内涵性、国际性、公益性、互动性和开放性；设立网络直播、微博、短信、现场提问等形式多样的互动平台；继续开展“寻找中国互联网的价值与潜质”的实地互动活动。

此外，在本次新闻发布会上，中国互联网协会与台北市电脑公会签署了合作备忘录，在本届中国互联网大会期间，将共同组织两岸移动互联网应用主题展览以及首届海峡两岸互动数字内容设计大赛决赛，以促进两岸互联网产业的交流与合作。

此次发布会吸引了国内多家知名互联网企业代表和各大新闻媒体。人民网、新华网、腾讯、搜狐、新浪、网易、第一视频、凤凰网等战略伙伴代表出席大会启动仪式。

高端容错计算机发展战略论坛在京召开

文章来源：中国信息安全博士网

【中国信息安全博士网讯】4 月 16 日，由 863 计划“高端容错计算机”重大项目总体技术专家组主办，哈尔滨工业大学、浪潮集团、中国电子信息产业发展研究院承办，中国建设银行、国防科技大学、华为技术有限公司、曙光信息产业有限公司、联想集团、赛迪顾问股份有限公司协办的“高端容错计算机发展战略论坛”今天在北京北辰五洲皇冠假日酒店隆重召开。

本次会议得到了科技部和许多单位的支持。科技部的相关领导对本次会议做了致辞；863 计划“高端容错计算机”重大项目总体技术专家组得左德承教授、IBM 公司硬件事业部战略合作部小型机架构 CTO：Michael Gebele 先生、中国建设银行总行高级架构师林磊明先生、Intel 公司英特尔关键业务服务器产品经理 Mike Demshki 先生、中国农业银行总行蔡仕志处长、法国国家科学院 Jean Arlat 高级研究员、HP 公司中国商业关键系统部总监 Robert Kennedy 先生、国家信息中心首席工程师宁家骏研究员、上海证券交易所技术中心副主任武剑锋先生、中国联通系统集成有限公司产品开发部副总经理高原先生、赛迪顾问计算机产业研究中心总经理孙会峰先生等专家做了主题演讲，分析了高端容错计算机技术的发展现状和应用安全，以及未来的技术方向和市场趋势。

本次会议主要讨论了高端容错计算机技术、产业、应用、发展战略等方面的内容。通过本次会议，进一步加强了我国在高端容错计算机技术方面的交流，也了解了当前国际社会再高端容错计算机技术方面的发展现状和趋势。

产业动态

Options Media 集团借道网秦进入手机安全市场

文章来源：CNET 科技资讯网

据 Marketwire 报道，移动营销市场和移动社交媒体市场的高速成长企业 Options Media 控股集团 (OTCBB: OPMG) 公布了一段该集团 CEO Scott Frohman 和 PhoneGuard 创始人 Anthony Sasso 参与的采访视频，视频采访可以在 www.joenoelstocks.com 上观看。

采访中，双方探讨了北美手机用户所面临的包括手机病毒和其他恶意软件在内的不断增长的安全威胁。还讨论了关于收购 PhoneGuard 获奖的防病毒和防恶意软件产品（该软件由网秦提供技术支持）的授权事宜以及这一合作将带来的成长机会。

Options Media 集团 CEO Scott Frohman 表示：“保护我们存储在手机上的数据变得越来越重要，我们认为使用 PhoneGuard 由网秦提供技术支持的产品是保护这些重要资产的最佳途径。现在北美的手机

用户刚刚开始认识到这些安全风险，而在亚洲和欧洲，数以百万计的手机用户已经安装使用这一防病毒软件。众多业内观察家认为北美市场即将迎来同样的爆炸性增长。在我们的视频采访中，我们探讨了这个市场的发展趋势和我们提议的许可证授权。随着我们产品线的不断扩张来满足移动社会媒体市场和移动营销/电子商务社区不断增长的需求，预计 Options Media 集团将迎来一个令人心动的时代。

4 月 1 日公布的合作意向书圈定了 Options Media 集团从北京网秦科技有限公司（此后简称网秦）取得北美市场再授权的基本条款。网秦为全球 200 多个国家和地区的超过 3500 万用户提供包括手机防病毒，防骚扰和隐私保护的服务，是手机安全领域无可争议的领导者。根据合作条款，Options Media 集团将会成为 PhoneGuard 软件套装（该软件套装由网秦提供技术和支持）在北美和加拿大的独家分销商，保护当地用户手机、PDA 以及智能手机免受黑客和网络犯罪的侵扰。

此外，Options Media 与 PhoneGuard 还达成一项口头协议，Options Media 将获取 PhoneGuard 由网秦提供的解决方案在美国和加拿大的再授权，该产品防止驾车者在驾驶时发送短信，这一行为目前在美国的 21 个州是被禁止的。PhoneGuard 计划在 4 月中发布这一产品。

蓝港王峰：王江民时代是技术天才大草莽时代

文章来源：腾讯科技

江民科技创始人王江民 4 月 4 日因病去世，享年 59 岁。蓝港在线 CEO 王峰撰文吊唁，称杀毒市场风云变换，有人令人恨，有人令人怕，但是王江民一直是圈子里令人敬重的人物。

王峰指出，那是一个真正的中关村英雄时代，在无奈和绝望中寻找希望，在万军中趁乱取得胜机。王江民的时代，是一个技术天才的大草莽时代。

据了解，王江民被誉为中关村最富有传奇色彩的知识英雄、中国软件业界中的奇才、国际上赫赫有名的“杀毒王”。

以下为蓝港在线 CEO 王峰撰文吊唁王江民：

王江民的辞世令人震惊。一下子心里沉了下来，想起了八年前杀毒市场风云。一个绝对的大哥级人物。一个技术市场两全的天才，一个属于中关村的时代。我还记得对他的印象，“有长者风范，说话很讲道理。”

深切怀念中国杀毒软件之父王江民老师。三足鼎立的杀毒软件时代，我在金山软件工作负责金山毒霸事业部，彼此打过很多交道。

我们虽然是曾经的市场同行和竞争对手的。但我是发自内心的尊重和佩服。杀毒市场风云变换，有人令人恨，有人令人怕，但是王江民一直是圈子里令人敬重的人物。

王江民，这三个字，在上个世纪最后十年里，中国盒装软件的黄金时代，几乎无人争锋。那是一个真正的中关村英雄时代，在无奈和绝望中寻找希望，在万军中趁乱取得胜机。王江民的时代，是一个技

术天才的大草莽时代。

江民科技后继有人 王江民之子接手管理

文章来源：腾讯科技

4 月 12 日，江民科技近日召开临时董事会，公司第二大股东、王江民前妻高宁在会上称，将支持王江民之子王营接手公司管理。

江民科技创始人兼董事长王江民上周突然辞世。持有公司 34% 股份的高宁在王江民的追悼会上表示，考虑转让全部所持股份，并离开杀毒行业。

据报道，高宁自己在 2004 年创办了北京飞客瑞康，从事数据恢复业务。她曾数次向王江民提出转让股份，但均被劝服。高宁 2001 年与王江民离婚，并于 2003 年左右淡出了江民科技，近年来江民公司的具体管理事务一直由总裁陶新宇负责。

以下为高宁公开信全文：

江民公司后继有人 大有希望

昨天，我和王营在缅怀江民的气氛中召开了江民去世后的第一次临时董事会，大家意见非常一致，就是继承江民的遗志，将江民的事业继续下去，我完全同意并坚决支持王营接手公司管理。

当王营告诉我“在爸爸遗物中发现爸爸精心保存阿姨和爸爸当年的照片和物品，我爸爸对您的感情很深”时，我控制不住自己的感

情，泪如雨下。初创时期的“小青蛙包装”和我们的工作照，都使我不能忘怀。

再次见到王营真的很吃惊，他太像王江民。经过多年精心的培养和国外良好的教育使他学业有成。王营主修工商管理兼修金融，已经成长为一个青年才俊，并且于 2008 年与品学兼优、秀美贤惠的妻子成婚，我看到这些感到无比的欣慰，相信江民在天之灵也会和我一样深感安慰。

江民的突然离去，给亲人们深重的打击，也使江民公司面临考验，但是我在见到王营的那一刻起，我就坚信自己的判断，这个年轻人他能行！他举手投足之间都透着和王江民一样的坚毅！非常理性异常坚强！不畏惧困难，勇于承担重任，我相信他！我会像当年辅佐他父亲那样坚定地支持他，得当处理当下事务，保持董事会高度一致，使他将全部精力投入到新江民的建设和发展中，光大王江民老师开创的事业。

同时，我也相信王老师留下的班子会支持王营，宣传王营，继续做好各自的工作。

高宁

2010-4-11

惠普成功收购 3Com 公司

文章来源：中国信息产业网

4 月 12 日晚间消息，惠普今天宣布其已经用现金以每股 7.9 美元的价格完成了对 3Com 公司的收购，涉资 27 亿美元，有关该交易的条款已获得惠普和 3Com 公司董事会的批准，3Com 旗下杭州华三通信技术有限公司(以下简称“H3C”)将正式并入惠普。

去年 11 月，惠普同意出价 27 亿美元并购 3Com，旨在拓展其产品组合、提高在快速增长的中国市场上的销售以及更好地与思科展开竞争。惠普可通过收购 3Com 丰富其产品，并可借助 3Com 的中国子公司而显著增强其在中国网络设备市场上的地位。

惠普会将 3Com 的网络产品和安全产品与其现有的 HP ProCurve 产品进行整合，从而为客户提供一个更全面的产品序列。借助惠普遍布全球的营销和服务资源，扩展后的产品序列将加固惠普的整合基础设施战略(该战略是以服务器、存储、网络、管理、工具和服务为基础进行构建的)。通过此整合，客户可以简化其网络并获得更全面的网络解决方案，增强其 IT 服务交付能力。

3Com 旗下的 H3C 拥有丰富的网络产品和解决方案，并在中国市场获得广泛成功应用。并购 3Com 后，惠普不仅可以扩展以太网交换机产品范围、增加路由解决方案，并且可以通过 H3C 显著提高惠普在中国的地位。另外，3Com 的 TippingPoint 产品组合可为惠普提供网

络安全功能。如此，惠普将成为能够提供市场上最广泛的网络产品及解决方案的供应商之一，进而在将来更好地满足客户的需求。

H3C 作为 3Com 的全资子公司，在交易结束后，将正式并入惠普。H3C 将全面负责中国大陆、香港和澳门的网络市场营销及服务。在中国以外的地区，惠普也将继续实施“China Out”战略，将 H3C 研发、生产制造的产品借助 HP 的全球资源更为广泛的在海外市场进行拓展和销售。

H3C 脱胎于华为，2003 年，华为与 3Com 在杭州合资成立华为 3Com，华为把中低端数据通信产品线纳入合资公司，并且运营团队也从华为整体调任。2006 年 11 月，3Com 以 8.82 亿美元成功竞购了华为手中 49% 的华为 3Com 股份，华为 3Com 也由此成为一家外商独资企业。

2007 年 4 月 27 日，华为 3Com 正式更名为杭州华三通信技术有限公司，企业标志也由“H3C”代替了“华为 3Com”，正式告别华为时代。

H3C 实际上就是以原华为员工为主要骨干，其发展非常快，2006 年，H3C 销售收入 7.12 亿美元，连续三年保持 70% 左右的同比增长。尤其是其擅长全线路由器和以太网交换机产品，目前是思科在华主要竞争对手之一，因此，业内认为，惠普收购 3Com 最主要的目的就是要将 H3C 收至麾下。

VB100 测试赛：国际大厂失手 中国杀软表现良好

文章来源：51CTO 译者：王文文

2010 年 4 月，VB100 杀软测试比赛落下帷幕。参赛的三个中国厂商的表现良好。令人感觉意外的是卡巴斯基一款产品（非个人版）的出局。

在此次比赛通过的国内产品有：

April 2010 - Kingsoft Internet Security 2010 Advanced Edition



Status: **PASS**
Product name: Kingsoft Internet Security 2010 Advanced Edition
More: April 2010 in full
Review: Kingsoft Internet Security 2010 Advanced Edition on Windows XP
Details: Only available to subscribers.

金山毒霸 2010 高级版

April 2010 - Kingsoft Internet Security 2010 Standard Edition



Status: **PASS**
Product name: Kingsoft Internet Security 2010 Standard Edition
More: April 2010 in full
Review: Kingsoft Internet Security 2010 Standard Edition on Windows XP
Details: Only available to subscribers.

金山毒霸 2010 标准版

April 2010 - Qihoo 360 Security



Status: **PASS**

Product name: Qihoo 360 Security

More: April 2010 in full

Review: Qihoo 360 Security on Windows XP

Details: Only available to subscribers.

奇虎 360 杀毒

April 2010 - Rising Internet Security 2010



Status: **PASS**

Product name: Rising Internet Security 2010

More: April 2010 in full

Review: Rising Internet Security 2010 on Windows XP

Details: Only available to subscribers.

瑞星 2010 版

在此次比赛出局的著名国外产品有：

April 2010 - Microsoft Security Essentials



Status: **FAIL**

Failure reason: 1 wildlist miss

Product name: Microsoft Security Essentials

More: April 2010 in full

Review: Microsoft Security Essentials on Windows XP

Details: Only available to subscribers.

微软 MSE

April 2010 - Kaspersky Anti-Virus 6 for Windows Workstations



Status: **FAIL**

Failure reason: 1 wildlist miss

Product name: Kaspersky Anti-Virus 6 for Windows Workstations

More: April 2010 in full

Review: Kaspersky Anti-Virus 6 for Windows Workstations on Windows XP

Details: Only available to subscribers.

卡巴斯基 Windows Workstations 6.0

在此次比赛出局的国内产品有：

April 2010 - Kingsoft Internet Security 2010 Swinstar Edition



Status: **FAIL**

Failure reason: 6 wildlist misses, 1 false positive

Product name: Kingsoft Internet Security 2010 Swinstar Edition

More: April 2010 in full

Review: Kingsoft Internet Security 2010 Swinstar Edition on Windows XP

Details: Only available to subscribers.

金山毒霸 2010 Swinstar 版

特别说明：

April 2010 - Avira AntiVir Personal



Status: **PASS**

Product name: Avira AntiVir Personal

More: April 2010 in full

Review: Avira AntiVir Personal on Windows XP

Details: Only available to subscribers.

小红伞个人免费版通过测试（2010 年初正式进入中国）。

注：本次所有测试平台为 Windows XP。

正日益扩大的外包安全服务业

文章来源：IT 安全

目前，各公司正在让安全管理服务提供商（managedsecurityserviceprovider, MSSP）负责更多的工作，而不仅仅是阻止垃圾邮件和加密邮件消息。非传统的外包安全技术正在升温，其中包括日志管理、补丁和配置管理等。

尽管 2009 年的经济动荡使得一些公司的安全预算停滞不前，但是安全服务市场依旧增长了大约 8%。Forrester 研究公司的副总裁兼首席分析师 KhalidKark 指出，这一增长未必都跟成本的消减有关。对于大多数企业来说，服务提供商所提供的每天 24 小时不间断保护以及安全管理能力的增强才是更重要的事情。

Kark 表示，“现在，各大公司发现安全威胁的频率和水平越来越高，本公司内部的人员已经无法控制，于是他们求助于那些能够提供帮助的服务提供商。IT 企业的组织结构开始变得异常复杂，企业中有些复杂性问题，一般的安全人员无法处理，但第三方可以处理这些问题，因为他们拥有更多的资源。”

最近，在 Forester 公司一个名为《市场概览：安全管理服务》的报告中，Kark 向人们展示了这个前景宽广的行业的发展方向，以及哪些公司应该寻求服务提供商的帮助。Kark 指出，企业应该努力寻找途径，按正确的优先顺序来投资，而不是削减成本。要做到这一

点，企业需要评估各种不同类型的 MSSP，包括那些把安全和通信服务捆绑在一起的电信提供商，以及提供混合服务的增值经销商和系统集成商。也有公司正求助于一些外包公司（如 IBM 和惠普公司）和安全产品供应商（如赛门铁克、McAfee 以及 VeriSign 等）。

FerrilliInformationGroup 的总裁兼首席执行官 RobertT.Ferrilli，在公司的交换服务器意外崩溃（在他出差期间）之后，就把公司所有的系统都外包给服务管理提供商。这家公司拥有一支具有 20 名开发人员的团队（他们遍布美国各地），主要是给各个大学和学院提供业务应用程序。虽然 Ferrilli 在公司内部部署了一些安全服务，但是他仍然委托 TriCipherInc. 公司为其网络应用程序提供单点登录功能。

Ferilli 说，“我对所有的维护和保养工作感到厌烦”。他认为数据包发送服务器失败是一件不可忍受的事情，这促使他把公司所有的系统都外包给云计算服务提供商。“这样我就可以专心管理我的生意，而不是去管理 IT 基础设施。”

Kark 呼吁大家在选择服务提供商的时候要谨慎。他表示，许多供应商都有许多服务套件，他们巴不得把所有的产品都卖给你，但是企业也要搞清楚到底想要从 MSSP 中得到什么，你需要制定一套固定的优先事项，这样才能够更好的判断什么样的合作伙伴真正适合自己。

Kark 指出，一开始的时候企业需要寻找几个值得信任的服务提供商，然后再决定他们所提供的服务以及产品能否跟公司的系统集成

在一起。Kark 表示，价格也应该作为判断的指标。有了多家供应商来参与竞争，企业才会有空间跟 MSSP 们讨价还价。

人们对非传统外包安全技术的兴趣正在升温

Kark 指出，这个行业正在经历一个转型期。企业正在从他们的 MSSP 那里寻求关于安全问题的指导，而不是仅仅得到网络过滤器或者电子邮件保护，这迫使一些公司投资建立咨询服务部门。

Kark 指出，email 和 Web 内容过滤器这样的内容安全技术仍然占据着大部分市场，但是其他的技术也在快速发展壮大。企业正在把日志管理服务、事件相关性与分析服务和分布拒绝服务保护外包出去。智能威胁报警服务、外包补丁管理和配置执行也变得流行起来。

随着云计算的普及，企业更多的数据将扩展到企业的防火墙之外，这也迫使一些公司寻求专业的安全机构来保护自己。Kark 表示，Symantec 公司的 MessageLabs、Google 的 Postini 服务以及 Zscaler Inc. 公司都有志于服务日益扩大的云安全市场。

Kark 说，“很多管理服务提供商正在把他们的服务更名为云服务”。有些电信运营商，包括 Verizon 以及 AT&T，可能更适合提供 DDoS 保护，但他们也提供基于云计算的 IPS 和 IDS 服务。

布鲁科特发布业界首个 IPv6 Web 安全网关

文章来源： 科技日报

布鲁科特系统公司(Blue Coat)日前发布了业界第一个 IPv6 Web 安全网关解决方案, 将应用、服务和内容自 IPv4 环境安全、无缝的迁移至 IPv6 环境。作为一个安全的 IPv6 应用迁移平台, Blue Coat ProxySG 设备可以利用 IPv6 技术优势帮助企业、政府部门及电信运营商削减成本, 提高效率。Blue Coat ProxySG 设备能够跨 IPv4 和 IPv6 应用及内容稳定执行企业 IT 策略。这一特性保证了企业的业务连续性, 而不会受到地址翻译相关问题的影响, 也不必重新编写应用或升级底层网络架构。

Blue Coat 解决方案的 IPv6 无缝部署能力, 帮助企业从 IPv4 的条条框框中解脱出来, 并在现有网络架构中部署和使用 IPv6 应用。通过在同一架构下对 IPv4 和 IPv6 混合应用的支持, 企业可以在不影响关键业务运行的前提下实现 IPv6 的技术优势。

瑞星杀软网络版新品正式发布

文章来源: IT 商业新闻网

4 月 15 日消息, 瑞星杀毒软件网络版新品今日正式发布。瑞星杀毒软件网络版分为小企业专用版、中小企业版、企业版、企业专用版、高级企业版、高级企业专用版、教育专用版等七个不同的版本。针对不同企业的特点, 瑞星杀毒软件可为企业提供对应的整体安全解决方案。

世界领先的“云安全”系统

瑞星“云安全”系统首次全面应用在企业级安全解决方案中，它通过互联网将 1.5 亿客户端（瑞星个人用户）与服务器实时连接，实时监测网络上出现的安全威胁，在最短时间内将解决方案瞬时送达客户端，并把其成果分享给 10 万家企业用户。

新一代瑞星反病毒虚拟机技术

新一代瑞星虚拟机应用分时技术和硬件 MMU 辅助的本地执行单元，在纯虚拟执行模式下，每秒钟执行超过 2000 万条虚拟指令，结合硬件辅助后，可以提高病毒的处理速度。

智能主动防御策略管理

使用全网智能管理功能，采用业界最强大的“木马入侵拦截”技术，全面防范网页挂马、U 盘等木马入侵途径。更有灵活的主动防御策略管理能力，网络管理员可以快速制定每个端点的主动防御规则，制定自己独有的防挂马、防木马策略，从而使得网络更加安全。

增强型日志查询报表系统

该系统为网络安全管理人员提供全面、细致、个性化、图形化的日志报表信息。自动生成定制的各种安全报告，实时掌控网络安全状况。网络管理员可轻松掌握每个端点的木马病毒感染情况、以及是否存在漏洞等安全隐患，彻底保障网络安全。

智能全网漏洞管理

作为微软全球 MAPP 重要合作伙伴，瑞星可以提前获取漏洞信息，

结合全新的漏洞扫描引擎，彻底修复网络安全漏洞。结合强大的全网管理功能，即时分类统计、汇总、备份，让网络管理员全面掌握、即时修补网络系统内的所有漏洞。

极速响应

网上出现的新病毒、木马样本提交到服务器后，基于“云安全”的病毒自动处理系统可以在最短时间内，对其进行智能分析和处理，并给出最终解决方案。95%的病毒样本可以在 5 分钟内处理完毕，帮助企业用户第一时间解决问题。

强大的网络管理功能是网络安全的基础

部署：针对国内复杂网络环境设计，轻松实现覆盖每台服务器和客户端的全网部署，支持 Web 安装、定制客户端安装包，提高全网安装效率。

管理：管理员可以对全网电脑配置木马查杀、主动防御、升级等功能。实时远程获取客户端安全信息，客户端按规则自动分组管理，自动获得防毒策略，管理员权限分级。

执行：在木马查杀、漏洞扫描、升级更新等日常工作中，分享“云安全”系统的安全成果，利用智能全网管理中心，大大提高网络管理员的工作效率。

游离升级：智能化识别虚拟升级服务器，通过远程身份认证技术，全面支持客户端的异地升级。彻底解决了游离客户端统一升级、统一管理的不便。

二次开发：针对国内网络及应用环境进行优化，提供全面的第三方二次开发接口，保证全网反病毒系统和其它管理、应用、安全软件的兼容和联动。

兼容多种平台

支持微软 64 位 Windows 平台，支持 Windows7、Vista 等各种主流 Windows、Unix、Linux 平台，适应国内多操作系统的复杂网络环境。携手全球一流厂商，率先推出软、硬件结合的安全解决方案。

一体化服务体系

200 名服务工程师为企业客户提供产品咨询、安装部署、技术支持及数据修复等服务。依靠强大的呼叫中心和客户服务平台，配合 7X24 小时新病毒应急响应部门，在短时间内为企业提供新病毒处理方案，解决各种网络安全问题。

ERM 为勘察设计企业知识产权保驾护航

文章来源：中国信息安全博士网

什么是知识产权

知识产权，英文为“intellectual property”，德文为“Gestiges Eigentum”，其原意均为“知识（财产）所有权”或者“智慧（财产）所有权”，也称为智力成果权。在中国台湾，则称之为智慧财产权。根据我国《民法通则》的规定，知识产权属于民事权利，是基于创造

性智力成果和工商业标记依法产生的权利的统称。有学者考证，该词最早于 17 世纪中叶由法国学者卡普佐夫提出，后为比利时著名法学家皮卡第所发展，皮卡第将之定义为“一切来自知识活动的权利”。

勘察设计公司知识产权的范围

勘察设计企业的知识产权保护范围可包括：

- 1、勘察设计成果文件的创作权；
- 2、设计竞选方案和自行编制的设计手册、企业标准、导则、手册、资料、通用图的版权；
- 3、单位的注册名称、商标及图形标志；
- 4、专利、专有技术和科研成果；
- 5、自编或二次开发的计算机应用程序和程序；
- 6、能带来收益的经营管理信息及需要保护的来自知识活动的权利等。

现代勘察设计公司知识产权的存在方式

知识产权是现代企业的生命，随着企业信息化程度的提高，企业的研发、生产等流程越来越依赖于信息系统。同时，企业的核心知识产权数字化程度也越来越高，这些核心知识产权形态是多样的，可能是设计文档、图纸或者其它文件的形式。由于数字化的知识产权具有容易复制、传输方便和形态多样的特点，为防止重要数据泄密，建立完善的安全保护体系，保护勘察设计企业的设计产品、重要的业务数据以及设计人员的劳动成果，最佳的做法是实施电子文档加密系统——

—思智 ERM。

勘察设计公司数据安全

思智泰克在思智 ERM 的基础上，经过长时间的调研和行业客户试用，研发了专门针对勘察设计企业的数据安全管理系统。它不但能够对 Microsoft Office 、 CAD 、 PDF 等任意格式的电子文档及设计图纸进行加密保护，并且能够对加密的文件进行细分化的应用权限设置和备份保护，确保勘察设计企业的机密数据只能被经过授权的人，在授权的应用环境中（例如企业内部），在指定的时间内，进行指定的应用操作，并且整个过程会被详细、完整的记录下来。

通过实施思智 ERM ，可以有效杜绝机密信息泄漏和窃取事件的发生，提升勘察设计企业的核心竞争力，优化流程，将管理的执行力度深入到数据信息的具体应用层面，从而推动勘察设计企业的发展。

金山成立安全子公司称将全面互联网化

文章来源：新浪科技

4 月 15 日下午消息，北京金山安全软件有限公司对外宣布成立，金山安全 CEO 王欣对外公布了未来两大核心战略：全面互联网化以及可信的云安全体系。王欣同时表示，金山安全不会做安全以外的其他产品。

根据此前媒体披露的资料，金山安全注册资本 800 万人民币，企

业法人雷军，今年春节后原金山毒霸安全业务副总裁王欣正式提升为金山安全软件 CEO。

金山安全未来战略时表示，金山不会做安全以外的其他产品，“金山安全的进一步发展是靠对安全的理解、技术以及服务实现，而不是以安全名义提供自己的互联网应用软件。”

金山安全今日发布包括金山毒霸 2011、金山网盾、金山卫士在内的全线安全产品，其中金山毒霸 2011 仍然是收费的专业安全软件，另外两款产品将永久免费。王欣表示金山安全未来两大核心战略是全面互联网化以及可信的云安全体系。

王欣此前在接受新浪专访时表示，金山安全将来不排除资本运作、上市的想法。因为本身安全是非常大的市场，而且国内也缺乏一家独立的自主创新的公司在本土，所以金山也是非常希望这块业务在国内能够包装上市。

瑞星“打黑”：力推云安全

文章来源：北京科技报

清晨，笔者像往常一样打开百度搜索引擎查询资料，几经尝试，却始终无法登录。事后记者才得知，原来百度被疑似来自伊朗的黑客攻击，无法正常访问，这是在 2010 年 1 月 12 日，百度所遭遇到的“黑网”事件。

随后，百度对外声明，从瑞星在第一时间内所检测到的故障，分

析出此次攻击黑客是利用了 DNS 记录篡改的方式。也正是由于瑞星的“火眼金睛”，在之后几个小时的时间内，百度随即恢复了正常。

现在，来自互联网的主要威胁正在由电脑病毒转向恶意程序及木马，有许多知名微博网站（Twitter）也遭遇到了类似的攻击，致使其首页遭到篡改。在这种情况下，用户往往寄托于杀毒软件的升级来保护自己的电脑。为了履行自己的职责，杀毒软件本身也在不断“求变”。瑞星就是其中的佼佼者，在继云计算、云存储之后，瑞星推出了云安全。

所谓“云安全”，指的就是融合了未知病毒行为判断等新兴技术和概念，通过对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。

采用云安全杀毒技术，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理。整个互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。

在瑞星新推出云安全的时候也并不是一帆风顺。它曾引起了广泛的争议，许多人认为它是伪命题。除了来自外界的质疑，内部对于它的技术路线也有不同的争论。

面对来自行业内外的各种声音，瑞星最后确定了打造“云安全”系统的策略。首先，瑞星打造的“云安全”必须要拥有海量的客户端，

这些客户端就相当于“探针”一样，它们是神经感知系统。一旦触摸出危险网站或者恶意程序，就会及时作出感知反应。一般而言，安全厂商的产品使用率越高，反应应当越快，最终应当能够实现无论哪个网民中毒、访问挂马网页，都能在第一时间作出反应。如今，瑞星已经拥有了近 1 亿的用户，庞大的客户群使得瑞星可以检测到互联网任何一个角落的风吹草动。

其次，需要专业的反病毒技术和经验。这些技术和经验都是需要时间累积而成的，它们是保护用户安全的引擎，恶意程序一旦被探测到，就会在最短的时间内被分析，否则容易造成样本的堆积，使云安全的快速探测的结果大打折扣。

再次，需要大量的资金和后台数据中心作为后备力量。“云安全”系统在服务器、带宽等硬件和技术团队等方面都需要极大的投入。目前在合作伙伴方面，瑞星现已有如搜狐、淘宝、支付宝、百度、中国移动、联想集团等知名企业的加盟。截至 2010 年 3 月，瑞星借助运行近两年的“云安全”系统，建成了国际领先、亚洲最大的病毒库，库内拥有 6000 多万个病毒样本，使用该库的瑞星杀毒软件，对于亚洲地区新出现的新增样本查杀率高达 95%。

此外，云安全的系统是一个开放的平台，允许有不断的合作伙伴加入，为云安全注入新鲜的血液。并且它还可以与其他软件相兼容，即使用户使用不同的杀毒软件，也可以享受“云安全”系统带来的成果。

此外，在一年的时间里，“云安全”成功拦截了 20 亿次挂马网站对用户的攻击，截获并处理了 2004 万个最新病毒样本。这些宝贵数据又被应用到了产品研发过程中，使瑞星的这个新产品全面解决了“病毒木马多途径传播”、“木马下载器泛滥”、“杀毒软件滞后于病毒”等三大业界难题。

在当今网络环境下，一家拥有 5000 名员工的企业，在已经部署了传统终端防护的情况下，一年内依然会有 2/3 的端点被感染，企业会因此而损失 250 万元的费用。与此同时，因为无法定位威胁的感染源头，病毒会在企业网络中不断重复感染，导致企业的损失被不断放大。

在 3 月 15 日，瑞星投资 1.3 亿元人民币的云安全数据中心正式启用。数据中心里有超过 5000 台服务器，能够为 10 亿用户提供高质量的安全检测、“云安全”信息交互及互联网威胁处理服务，对绝大多数病毒文件的自动分析处理可缩短到 1 秒，将保护用户安全的时间几乎提到了实时同步的程度。

随着互联网应用的深入，很多用户遇到的并非单纯的病毒问题、木马问题，而是综合了社会工程欺诈、网络钓鱼心理学、网络犯罪和网站挂马等一系列的新型技术和手段，原本的杀毒软件无法应对此类需求，而瑞星的“云安全”系统正是应运而生。

假冒杀毒软件增长 占恶意在线广告的 50%

文章来源：中国安全 作者：天虹

据谷歌即将发表的一篇报告称，假冒的杀毒软件正在增长，目前大约占检测到的全部恶意软件的 15%。

假冒的杀毒软件一般都假装对受害者的计算机进行扫描并且声称发现一些恶意软件。这时，假冒的杀毒软件要求用户付费以便清除这个不存在的恶意软件。无论用户是否付费，这个假冒的杀毒软件都可能安装更多的恶意软件。

谷歌对这个话题感兴趣的原因在于：计算机用户经常通过垃圾信息网站和在线广告联系上假冒的杀毒软件。除了担心保持用户的信任和安全之外，谷歌要保证在线广告不能成为广泛应用的传播恶意软件的手段。否则，用户就会拒绝合法的广告，把合法的广告当作一种风险。

谷歌即将发表的题为“网络的反安慰剂效应：假冒杀毒软件传播分析”的报告称，在过去的 13 个月里，谷歌发现有 1.1 万个域名参与了发布假冒的杀毒软件。假冒杀毒软件攻击占网站上发现的恶意软件的 60%。这篇报告称，假冒的杀毒软件占通过在线广告传播的全部恶意软件的 50%，比一年前增加了五倍。

病毒播报

本周病毒预报（4.12——4.18）

文章来源：信息安全司

国家计算机病毒应急处理中心通过对互联网的监测发现，微软公司将会在下周二发布 11 个漏洞补丁程序，修复其开发的操作系统和应用软件所存在的多个漏洞，这些系统和软件包括 Windows 操作系统、办公自动化处理软件 Office 和邮件系统 Exchange 等。在发布的这些漏洞补丁程序中，有 5 个补丁程序的危害等级会是严重级别，这些严重的漏洞可能使恶意攻击者远程控制被入侵的计算机操作系统。

在这些漏洞补丁程序中，特别值得注意的是微软公司将修复两个漏洞，这两个漏洞都是在微软公司已经公布了的安全公告中提及到的，而事后并没有发布针对该漏洞的补丁程序。这两则公告分别是编号 981169 和编号 977544。

1、在安全公告 981169 中指出：在使用浏览器 IE 时，脚本程序与 Windows 帮助文件在交互的方式上存在漏洞。一旦恶意 Web 网站中弹出特制的用户对话框且计算机用户按了键盘 F1 帮助键，那么恶意攻击者可以远程在操作系统中执行任意代码。该漏洞涉及 Microsoft Windows 2000、Windows XP 和 Windows Server 2003 这几个版本。

2、在安全公告 977544 中指出：SMB（服务器消息块）协议中允许实施拒绝服务攻击。此漏洞不能用于在计算机用户操作系统上控制

或安装任意恶意软件。

专家提醒：

针对以上情况，国家计算机病毒应急处理中心建议广大计算机用户注意浏览微软公司的官方网站，一旦这些漏洞补丁程序被发布出来，应及时下载安装到操作系统中，防止恶意攻击者利用这些漏洞来入侵感染操作系统，避免操作系统遭受到远程恶意攻击的威胁。

技术前沿

曲成义：信息安全的理解和全局对策

文章来源：信息安全协调司

面对信息化的高速发展，信息安全面临着极其严峻的形势。国家信息化专家咨询委员会曲成义站在全局的高度，深刻剖析了信息安全的四大特征和难点，指出了信息安全需创建的四种能力和“六性”，并从信息安全的顶层设计出发，总结出四项全局对策。

一、信息安全要创建“四种能力”

1. 构建完善的信息安全基础设施，为信息安全提供公共的支撑能力：如建立由数字认证、安全测评、网络监控、事件通报、应急支援、灾难恢复、舆情治理等信息安全基础支撑平台和支撑体系。

2. 提升信息安全的防护与对抗能力：信息安全的攻与防是一个过程，要在预警、监测、防护、恢复、反击等过程的各个环节都采取有效的对抗手段，才能奏效。

3. 建立应对网络突发灾难事件的应急和容灾能力：当网络突然灾难事件来临时，要启动应急预警，采取灾难恢复机制，即使全系统毁灭，也能在异地即时恢复信息系统的使用，保持业务的可持续性。

4. 强化信息安全管理可控能力：鉴于信息系统的复杂性和使用行为的多样性，单靠技术手段是不能完全奏效的，必须动用管理可控手段，双管齐下，所以信息安全的对策是技术与管理手段并用。

二、信息安全要保障信息及其服务具有“六性”

这“六性”包括：信息的“保密性”、信息的“完整性”、系统及服务的“可用性”、信息内容及主体行为的“可核查性”、主客体身份的“真实性”，主体行为和信息内容的“可控性”。

三、果断推进信息安全的全局对策

1. 落实信息安全的等级保护制度

在信息安全投入（资金、人力、资产等）与系统所能承受的最小风险之间找到科学的平衡点，保护国家、社会的最大利益。

2. 构建网络信息系统的“信息安全保障体系”

根据信息系统的安全等级，依据国家已发布的相关标准和规范，在作好信息系统安全需求分析的基础上，构建或者调整网络信息系统的信息安全保障体系，重点抓好：①网络纵深防御体系的设计、安全

域的科学划分和安全边界的有效隔离；②网络动态防护机制设计，安全机制能在安全对抗的全生命周期过程中有效协同和对抗；③建设好基于密码技术的网络信任体系，包括身份认证、授权管理和责任认定。④强化内部审计，从网络级、数据库级、系统级、主机级和介质级的全局审计入手，并逐渐使审计点前移；⑤建设好信息系统的“信息安全管理体系”（ISMS），遵从 PDCA 模型，不断优化 ISMS。

3. 抓好信息安全测评的风险评估工作

鉴于网络信息系统是一个“复杂巨系统”，其信息安全检测与风险评估是一项“系统工程”，在重视培育自评估能力的同时，要重点通过专业的第三方（行政检查评估或服务委托评估），及时发现隐患，采取对策，调整系统，提升强度，与所确定的安全等级相匹配。

云的安全和云安全

文章来源：经理世界网

29 岁的黄亮是上海一家外企职员，平时爱好旅游和摄影。最近，让黄亮心里“长草”的是中国电信新推的一项业务——E 云。

“E 云”提供的是一项基于云计算的互联网备份服务，每月缴纳 40 元钱就能拥有 300G 的超大存储空间。“这样在旅途中就不用带那款笨重的笔记本，照片随时通过小上网本传到网上存起来，费用也可以接受。”黄亮想想不禁有些兴奋。

“在安全方面，您的数据只归您个人所有，其他任何一方，包括中国电信都无权访问您的私有数据。”客服人员的信誓旦旦不但没有打消黄亮的最后一丝顾虑，反而让他想到一个问题：把散落在两个笔记本和几块移动硬盘里的文件集中储存在“云”端，可就是把所有鸡蛋放在一个篮子里了！黄亮不敢想象自己走遍各地拍摄的心血之作一旦有失，或者自己为女友拍摄的艺术照外泄的结局会怎样，他又犹豫了。

让黄亮犹豫的正是目前云计算在全球面临的一块短板——安全。随着云计算应用种类和范围的不断扩大，越来越多的企业和个人的关键信息被集中到“云端”，因此云计算系统中安全漏洞的价值也越来越受到黑客们的重视。另外，由于电子邮件、即时通信、SNS、博客等应用的交叉相关性，一个账户被破解往往带来连锁反应，相当于把“串好”的鸡蛋放在了一个篮子里，更容易被一扫而光。

2009 年底，Twitter 公司某管理人员的个人电子邮件被黑客入侵，黑客利用邮件中的信息访问了该员工的 Google Apps 账户，最终窃取了 Twitter 公司的大量文件，从各种创意文案到详细的财务资料一应俱全。很快，一份包含 310 份 Twitter 机密文件的压缩包开始在网上公开叫卖。

云计算服务以简洁、廉价著称，在全球赢得了众多拥趸，但“云”的安全问题始终如阴影围绕左右。在屡次发生大规模资料泄露事件之后，人们发现在公有云中，某些应用程序被关在了防火墙的外面；另

外,用户账户的糟糕配置也让黑客能够轻松访问云的内部。在理论上,解决“云”的安全的最有效方法当然是像 IBM 等大企业,建立私有云架构来保存机密信息,但这显然缺乏可操作性。

2010~2013年全球安全产品营收预期 (按平台类型分) 单位:百万美元					
平台	2010 年	2011 年	2012 年	2013 年	2010-2013 年复合增长率 (%)
软件	16330.1	17576.7	18691.6	20038.3	7.1
硬件	9308.0	10192.3	1106.4	11932.8	8.6
虚拟化	433.8	667.6	1040.5	1492.6	51
SaaS	2185.7	2790.6	3534.6	4315.8	25.5
总计	28257.6	31227.2	34383.1	37779.4	10.2
数据来源: IDC					

2010~2013年全球安全产品营收预期 (按细分市场分) 单位:百万美元					
细分市场	2010 年	2011 年	2012 年	2013 年	2010-2013 年复合增长率 (%)
终端	7085.9	7713.3	8582.3	9583.9	10.6
邮件	3459.5	3882.7	4309.1	4747.1	11.1
Network	8185.3	9036.6	9786.7	10530.4	8.8
Web	1811.2	2079.2	2347.0	2617.0	13.1
身份识别及访问管理	3674.0	4201.0	4497.0	4814.0	7.5
安全及漏洞管理	3048.4	3432.1	3880.0	4393.4	13.0
其他产品	793.3	882.3	981.0	1093.6	11.3
总计	28257.6	31227.2	34383.1	37779.4	10.2
数据来源: IDC					

云计算以及相关安全问题,为赛门铁克、McAfee、趋势科技、卡巴斯基、瑞星、360 等安全厂商带来的不仅是新的市场机遇,更在应用技术和商业模式上革了杀毒软件们的命。

但事实上,中国用户对“云计算”的了解和熟悉,恰恰是通过业界在 2008 年开始高调宣传的“云安全”(Cloud Security)完成的。

“云安全”一词是中国杀毒企业创造的概念,是云计算在安全领域的具体应用。具体来讲,就是将病毒的采集、识别、查杀、处理等行为全部放在“云”端,基于互联网对与此连接的终端的安全信息进

行处理。将病毒库设置在“云端”，利用云计算架构收集和分发病毒代码，对互联网网页以及文件进行信誉评级，可以减轻运行庞大病毒库给终端系统带来的负担，加快病毒库的更新速度。

从“买盒子”进化到“买服务”，云计算为安全领域带来的商业模式变化，并不局限于在线付费，更加拓宽了杀毒软件们提供安全服务的范围和层次——免费提供在线查毒（同样基于云计算）、有限杀毒等低端服务；对全面防护、网络存储等高端服务收费。这种免费与收费混搭的策略正是克里斯·安德森在《免费》一书中提出的未来商业模式：免费平台+增值服务。在中国，周鸿祎的 360 杀毒将安全这项互联网基础服务推上了免费的终极跑道。

提供“云安全”，如同提供其他云服务一样，对厂商在客户数量及硬件投入方面都有很高的要求。比如病毒采集，只有拥有海量的客户端，才能对互联网上出现的恶意程序，危险网站有最灵敏的感知能力。一般而言，安全厂商的产品适用范围越大、使用率越高，对病毒和木马攻击的反应则越快。另外，实现“云安全”之初需要在服务器、带宽等硬件方面投入极大，同时要求安全厂商应当具有相应的顶尖技术团队、持续的研究经费。

威胁隔离！用 SELinux 保护虚拟化

文章来源：51CTO 翻译：黄永兵

虚拟化被认为是计算机技术发展史中的一次技术革命，它在资源分配，系统管理，电力和制冷成本节省，按需扩大或收缩资源等方面表现出极大的优势，虽然人人都在谈虚拟化，人人都准备用上虚拟化，但一直伴随虚拟化挥之不去的阴影 - 安全问题 - 又让无数人望而却步。

虚拟化安全性如何？

当攻击者攻破虚拟机，接管了虚拟机的所有控制权后会发生什么？如果系统管理程序（Hypervisor）存在 bug 又会发生什么？

在未虚拟化之前，我们隔离了服务器，攻击者攻破一台服务器后，他只能控制那一台服务器，这时攻击者必须采取网络攻击，攻击网络内的其它服务器，才有可能拿到其它服务器的控制权。系统管理员有很多工具检测和保护网络攻击，如防火墙，网络流量分析工具，入侵检测工具等。

虚拟化后，在同一台物理主机上运行了多个服务（应用程序），如果虚拟机被攻破，攻击者只需要破坏系统管理程序，就可以达到破坏所有服务的目的。如果系统管理程序存在漏洞，攻击者可以接管主机上托管的所有虚拟机，甚至可以向主机能直接访问的虚拟机镜像写入恶意代码。

听起来非常恐怖吧，现在的问题是如果真发生这种情况时该如何处置，攻击者对系统管理程序的漏洞兴趣越来越浓，前不久 Xen 系统管理程序就已经被攻破了。——51CTO 王文文：VMware 的产品中同样

出现过类似问题，而现在他们已经在采用 RSA 的身份认证技术来缓解虚拟数据中心威胁了。那如果不使用身份认证技术的话，我们看看本文中 SELinux 的保护方式。

现在我们来看看 Fedora 11 中的 libvirt/qemu/kvm，libvirt 启动所有虚拟机，所有虚拟机都以独立的进程运行，虚拟镜像被保存为一个文件或类似逻辑卷和 iSCSI 目标的设备。

SELinux 真的有用么？

SELinux 标记进程，文件和设备，同时负责定义被标记进程，文件和设备之间互操作的规则，通过 SELinux 可以减小系统管理程序漏洞引起的影响范围。

如果你阅读过 Xen 漏洞文档，你一定知道如何绕过 RHEL 5 中 SELinux 保护机制，攻击者知道标记为 `xend_t` 的 `xen` 进程可以读/写所有用 `fixed_disk_device_t` 标记的固定磁盘，通过写物理磁盘，攻击者可以绕过 SELinux 的限制。我给 RHEL 5 上的 Xen 编写策略时，最初要求管理员将 Xen 镜像设备卷标记为 `xen_image_t`，Xen 开发人员认为这对管理员的管理来说太困难了，可能会导致许多故障，我们没有时间制作管理工具使其自动化，大家都认为在这个例子中可用性比安全更重要，我不得不同意他们的意见。

在 Fedora 11 中，James Morris，Daniel Berrange 和我以及其它共事者给 libvirt 增加了 SELinux 支持，形成了 sVirt，我们给 libvirt 增加了一个插件架构，默认启用了 SELinux 保护，理论上你

可以使用其它安全架构。libvirt 动态地标记镜像文件，并用正确的标记启动虚拟机，管理员不必记住给镜像文件和设备设置的标记，在 F11 中，默认所有虚拟机都使用 `svirt_t type` 类型标记，所有镜像文件都使用 `svirt_image_t` 类型标记。

SELinux 策略规定 `svirt_t` 进程可以读/写 `svirt_image_t` 文件和设备。

这种保护允许我们保护主机不受任何虚拟机的侵害，虚拟机只能与正确标记的文件和设备交互，被攻破的虚拟机不能访问我的 home 目录，即使虚拟机以 root 权限运行。

但这种类型的保护不能阻止一个虚拟机攻击另一个虚拟机，我们需要一种方法使用相同的类型标记域和镜像文件，与此同时，停掉虚拟机 1，以 `svirt_t` 类型运行，攻击虚拟机 2，虚拟机 2 也将以 `svirt_t` 类型运行。

多类别安全 (Multi Category Security, MCS) 保护

我们在开发 RHEL 5 时，我们增加了 MCS 支持，包括给 SELinux 上下文增加第四个字段。

最开始在 RHEL 4 中，SELinux 上下文只有三个字段：“用户:角色:类型”，在 RHEL 5 中，SELinux 上下文字段增加到四个：“用户:角色:类型:MLS”，例如，home 目录中的文件可能被标记为 `system_u:system_r:user_home_t:TopSecretRecipe`，MLS 标记定义了一个敏感级别 (s0-s15) 和数据分类 (c0.c1023)，这个例子中的

TopSecretRecipe 是类似 s15:c0.c36 这样的字段的人文翻译,MLS 标记允许 MLS 机器不仅可以基于它的使用者标记文件,在这个例子中是 user_home_t, 也可以根据敏感性和内容的本身属性进行标记,如 TopSecretRecipe。

这个字段仅在 MLS 策略中使用,我们尝试在默认策略(targeted)中使用它,只定义一个敏感级别(s0),允许管理员定义分类,我们把它叫做多分类安全(MCS),旨在让管理员和用户可以根据文件内容的自身属性进行标记,如

system_u:object_r:database_t:PatientRecord 可能是一个包含病人记录的数据库,遗憾的是,由于种种原因,MCS 未被广泛使用。

但我们在开发 sVirt 时,我们认识到可以使用 MCS 隔离两个相同 SELinux 类型(svirt_t)的虚拟机,我们设计 libvirt 分配一个不同的随机选择的 MCS 标记给每个虚拟机及其关联的虚拟镜像,libvirt 保证它选择的 MCS 字段的唯一性,SELinux 阻止以不同 MCS 字段运行的虚拟机互操作,这样就保证了虚拟机不会相互攻击。

例如,libvirt 用下面这些标记创建两个虚拟镜像:

名称	虚拟机进程标记	虚拟机镜像标记
虚拟机 1	system_u:system_r:svirt_t:s0:c0,c10	system_u:object_r:svirt_image_t:s0:c0,c10
虚拟机 2	system_u:system_r:svirt_t:s0:c101,c230	system_u:object_r:svirt_image_t:s0:c101,c230

SELinux 阻止虚拟机 1(system_u:system_r:svirt_t:s0:c0,c10) 访问虚拟机 2 的镜像文件

(system_u:object_r:svirt_image_t:s0:c101,c230)，因此这两个虚拟机不能互相攻击。

下面是 libvirt 指定的标记：

名称，	SELinux 上下文，	描述，
虚拟机进程，	system_u:system_r:svirt_t:MCS1，	MCS1 是一个随机选择的 MCS 字段，目前我们支持约 500000 个标记，
虚拟机镜像，	system_u:object_r:svirt_image_t:MCS1，	只有有相同 MCS 字段的 svirt_t 进程可以读/写这些文件和设备，
虚拟机共享的读/写上下文，	system_u:object_r:svirt_image_t:s0，	所有 svirt_t 进程都允许写 svirt_image_t:s0 文件和设备，
虚拟机共享的只读上下文，	system_u:object_r:svirt_content_t:s0，	所有 svirt_t 进程都可以读该标记的文件/设备，
虚拟机镜像（复数），	system_u:object_r:svirt_content_t:s0，	当虚拟机存在时，它的镜像文件使用系统默认值标记，通常是 virt_content_t:s0，非 svirt_t 虚拟进程可以读/写该标记的文件/设备，

我们也给 sVirt 增加了静态标记的功能，静态标记允许管理员为虚拟机选择一个特殊的标记，包括 MCS/MLS 字段，虚拟机将总是以这个标记启动，运行静态虚拟机的管理员负责给镜像文件设置正确的标记，libvirt 永远不会修改静态虚拟机上下文的标记，它允许 sVirt 组件在 MLS 环境下运行，你可以在一个 libvirt 系统上以不同敏感级运行多个虚拟机。

云计算与网络计算 基于网络的不同技术

文章来源：ZDNET 网络频道

目前，全球 IT 行业正在进行着一场浩浩荡荡的“云”端之旅。

《商业周刊》最近发表评论文章指出，云计算技术的出现使得人们可以直接通过网络应用获取软件和计算能力，这模式将会给传统的 IT 业带来一场巨大的变革，云计算正在成为 IT 业的一种发展趋势。尽管云计算的定义和范围目前尚无定论，存在多方说法和理解。但是毫无疑问的是。它的影响将逐渐地渗透到人们的工作和生活之中。随着互联网连接速度的提高和互联网软件的改进，云计算能够完成的任务会越来越多。

可能大家首先会问的是什么是云计算。应该说，云计算(Cloud Computing)是分布式处理(Distributed Computing)、并行处理(Parallel Computing)和网格计算(Grid Computing)的发展，或者说是这些计算机科学概念的商业实现。

云计算的基本原理是，通过使计算分布在大量的分布式计算机上，而非本地计算机或远程服务器中，企业数据中心的运行将更与互联网相似。这使得企业能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。

目前，PC 依然是我们日常工作生活中的核心工具：我们用 PC 处理文档、存储资料，通过电子邮件或 U 盘与他人分享信息。如果 PC 硬盘坏了，我们会因为资料丢失而束手无策。而在“云计算”时代，“云”会替我们做存储和计算的工作。“云”就是计算机群，每一群包括了几十万台、甚至上百万台计算机。“云”的好处还在于，其

中的计算机可以随时更新，保证“云”长生不老。

网格计算技术

但另一方面，我们不能不提及目前正在使用的网格计算技术，网格是通过局域网或广域网提供的一系列分布式计算资源，而对终端用户或应用来讲，好像是一台大型虚拟计算机。这种构想是通过在个人、组织和资源之间实现安全、协调的资源共享，来创建虚拟动态的组织。网格计算是分布式运算的一种方法，不仅包括使置，而且还涵盖组织、硬件和软件，以提供无限的能力，使连接到网格的每个人都可以进行合作和访问信息。网格计算同样也是应用于分布式运算的一种方法，但是可以说从很多方面比较，云计算都是网格计算技术的一次飞跃。

云计算与网格计算的比较

首先，我们可以从网格计算的作业调度方面来进行比较。作业调度是网格技术的核心价值，网格的目标，是想要尽可能地利用各种资源。它通过特定的网格软件，将一个庞大的项目分解为无数个相互独立的、不太相关的子任务，然后交由各个计算节点进行计算。即便某个节点出现问题，没有能够及时返回结果，也不影响整个项目的进程，甚至即便某一个计算节点突然崩溃，其所承担的计算任务也能够被任务调度系统分配给其他的节点继续完成。

而云计算也像网格计算一样将所有的资源构筑成一个庞大的资源池，但是云计算向外提供的某个资源，是为了完成某个特定的任务。比如，某个用户可能需要从资源池中申请一定量的资源来部署其应用，

而不会将自己的任务提交给整个网络来完成。从这一点来看，网络的构建大多为完成某一个特定的任务需要，这也是会有生物网格、地理网格、国家教育网格等各种不同的网格项目出现的原因。而云计算一般来说都是为了通用应用而设计的，没有专门的以某种应用命名的网格。

其次，云计算将在三大方面产生 4 响：对互联网应用的影响、对产品应用模式的影响、对 IT 产品开发方向的影响。当然，所谓的改变并不是彻底的颠覆，而是增加了新的特点。这一优势，是对网格技术提出的挑战。网格计算产生时同样具有以下优势：通过任何一台计算机都可以提供无限的计算能力，可以接人浩如烟海的信息。这种环境将能够使各企业解决以前难以处理的问题，最有效地使用他们的系统，满足客户要求并降低他们计算机资源的拥有和管理总成本。

但对于云计算来说，是对这些优势的更大扩展。今后通过云计算，更多地应用能够以互联网服务的方式进行。云计算将扩大软硬件应用的外延并改变软硬件产品的应用模式。通过云计算，用户可以不必要购买新的服务器和部署软件，就能得到应用环境或者应用本身。对于用户来说，软硬件不必是部署在自己身边的、专属于自己的产品，而是可以变身为可利用的、虚拟的一种资源。而且，可以利用的软硬件资源也不仅限于自己企业内部的设备和软件，而是可以通过网络得到扩展的软硬件资源。IT 产品的开发方向也将发生变化，以适应上述两种情况。

四步预防恶意软件威胁

文章来源：IT 专家网

恶意软件被认为是当今企业面临的最大的、发展最迅速的安全挑战，在对 IT 专业人士的最新调查显示，超过 32% 的 IT 人士认为在未来 12 个月内安装在个人电脑中的恶意软件必将对 IT 安全造成巨大外部威胁，超过 16% 认为移动设备上的恶意软件也将造成威胁。总而言之，个人电脑和移动设备中运行的恶意软件被认为是 2010 年最大威胁。

以下是对恶意软件威胁类型的说明，以及企业应该如何部署安全策略保护企业自身安全的技巧。

恶意软件威胁

近年来，企业一直在与恶意软件作斗争，但威胁仍然在不断演化，其中企业面临的最大问题就是个人信息泄漏。攻击者们开始广泛部署复杂恶意软件来窃取合法用户的用户名和密码，他们可以通过多种方式进行窃取，包括用户无意安装恶意软件、浏览器恶意软件和窃听攻击等。

例如，在 2009 年 11 月，一名安全专家就利用 SSL(安全套接字层)协议的漏洞成功获取 Twitter 用户的登陆信息，可能大家会认为这种攻击不太会造成伤害，但请考虑一下，有多少人会使用与 Twitter

帐号相同密码作为网上银行登陆密码呢?有多少企业用户会使用相同密码来登陆企业域呢?这些各种形式的恶意软件可能通过各种方式引发安全泄漏事故。

另外一种攻击媒介就是最近报道的针对 SSL VPN 使用浏览器恶意软件来登陆已在浏览器登陆过的帐户。这种攻击利用了大多数 SSL VPN 与浏览器的同源政策交互的方式,这样很容易致使用户泄漏密码,当他们使用浏览器登陆企业邮箱帐户时。

另一种恶意软件相关的威胁涉及针对性钓鱼攻击。我们看到越来越多的攻击者通过发送精心制作的钓鱼电子邮件信息来攻击用户,这些电子邮件信息可能包含恶意软件(以安装在用户电脑)或者恶意网站链接。可以说,这些钓鱼攻击方式的高度针对性让一般用户很难检测,最新试验证明,包含假冒社交网站链接确实能够成功让用户点击并安装恶意软件。

最后,信息盗窃是新一代恶意软件主要涉及的攻击活动。像 Clampi 和 Zeus 这种木马病毒能够主动窃取信息,并且可以窃取任何攻击者感兴趣的信息。例如,它们可以窃取登陆网上银行的用户名和密码,更糟的是,它们可以创建隐藏交易,让用户将钱转到攻击者控制的银行帐号。传统的身份验证解决方案(例如令牌和智能卡)对于预防这种攻击都没有用。

预防恶意软件威胁的四步骤

主要有以下四个步骤可以帮助大家预防企业内的恶意软件威胁：

第一步：部署企业反恶意软件解决方案

随着恶意软件逐渐成为安全机制的核心问题，企业都应该部署自己的防恶意软件解决方案，并且由于大多数恶意软件都会直接影响用户电脑，因此安全重点应该是企业中每台用户计算机。

此外，由于远程访问技术无处不在，远程用户也应该部署相同的安全措施，最好就是为远程用户部署完成的端点安全解决方案，包括修补程序和防火墙管理以及防恶意软件程序。最后，可以考虑部署入侵防御系统 (IPS) 来拦截和预防某些由远程用户导致的攻击。

第二步：及时修复

由于安全领域技术日益变化，企业应该随时保持企业系统的更新状态，例如可以专门安排一名工作人员关注 CERT 警告和漏洞标签以获取任何更新信息，保持企业系统的及时修复可以在很大程度上降低安全风险。当然有时供应商的修复补丁可能会比较晚，但及时修复补丁绝对是最安全的做法。

第三步：部署强大的身份验证机制

很多企业攻击都是依靠单一验证而发动攻击的，传统钓鱼式攻击、键盘记录攻击以及上述 Twittr 攻击都属于这种形式。这些攻击主要在于窃取个人信息 (用户名和密码)，这些信息将用于登陆用户的帐户。部署额外的身份验证机制可以抵御这些攻击，例如通过要求用户使用

自身的东西(安全设备)或者指纹等来验证身份。部署多因素身份验证系统通常能够抵御上述所有攻击形式。

因为这些攻击可以获取信息,例如用户安全问题的答案,额外的基于信息的身份验证并不能提供额外的保护,数字证书也是同样的道理,因为这些信息都很容易复制或者窃取,并不能抵御这些攻击。

目前选择身份验证解决方案的最佳做法是,选择一个带外双因素系统,因为现在的恶意软件已经能够攻击传统的带内双因素系统。另外,考虑添加生物认证因素,混合声音、指纹或者其他三因素验证系统。通过使用单独渠道(例如电话网络)进行第二层验证,还可以帮助避开安装在用户设备上的恶意软件。

第四步: 使用通信验证

如果你在银行工作,你应该需要注意一种新型恶意软件威胁,这种攻击形式等待用户登陆然后通过 SSL 渠道在用户完全不知情的情况下将选择的交易发送给攻击者。

这些攻击完全可以通过带外交易验证系统来抵御,不管用户什么时候发起一个交易(或者只是选定的交易),银行会自动打电话给用户的注册电话号码,将拟定进行的交易详情告诉用户,只有当用户批准的情况下才能继续进行交易,这样可以避免恶意软件的恶意行为。

探析网络安全与防范技术

文章来源：中国电子商务研究中心

1. 影响网络安全的几个方面

1.1 计算机病毒的内涵

计算机病毒：指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

计算机病毒虽是一个小程序，但它和别的计算机程序不同。具有以下特点：

①计算机病毒的程序性：它是一段可执行程序，但它不是一个完整的程序，而是寄生在其他可执行程序上；②计算机病毒的传染性：是病毒的基本特征，计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机。③计算机病毒的潜伏性：一个编制精巧的计算机病毒程序，进入系统之后可以长时间的隐藏在合法文件中。对其他系统进行传染；④计算机病毒的可触发性：病毒因某个事件会诱使病毒实施感染或进行攻击的特性；

1.2 网络资源共享性因素

资源共享是计算机网络应用的主要目的，但这为系统安全的攻击者利用共享的资源进行破坏提供了机会。随着联网需求的日益增长，外部服务请求不可能做到完全隔离，攻击者利用服务请求的机会很容

易获取网络数据包。

1.3 网络开放性因素

网上的任何一个用户很方便访问互联网上的信息资源，从而很容易获取到一个企业、单位以及个人的敏感性信息。

2. 网络安全防御方式

防火墙作为一种边界安全的手段，在网络安全保护中起着重要作用。它使得内部网络与因特网之间或与其它外部网络之间互相隔离、限制网络互访，用来保护内部网络。

2.1 防火墙的主要功能

①防火墙可以对流经它的网络通信进行扫描，从而过滤掉一些攻击；

②防火墙可以关闭不使用的端口，而且它还能禁止特定端口的输出信息；

③防火墙可以禁止来自特殊站点的访问，从而可以防止来自不明入侵者的所有通信，过滤掉不安全的服务和控制非法用户对网络的访问；

④防火墙可以控制网络内部人员对 Internet 上特殊站点的访问；

⑤防火墙提供了监视 Internet 安全和预警的方便端点。

2.2 防火墙的主要优点

防火墙可作为网络通信的阻塞点。所有进出网络的信息都必须通过防火墙。防火墙承担风险的范围从整个内部网络缩小到组成防火墙

系统的一台或几台主机上。从而在结构上形成了一个控制中心，极大地加强了网络安全，并简化了网络管理。

2.3 防火墙的主要缺陷

由于互联网的开放性，防火墙也有一些弱点，使它不能完全保护网络不受攻击。防火墙的主要缺陷有：

①防火墙对绕过它的攻击行为无能为力；

②防火墙无法防范病毒，不能防止感染了病毒的软件或文件的传输，所以对于以上提到的计算机病毒只能安装反病毒软件。

2.4 防火墙的分类

防火墙的实现从层次上大体可分为三类：包过滤防火墙，代理防火墙和复合型防火墙。

2.4.1 包过滤防火墙

包过滤防火墙是在 IP 层实现，它可以只用路由器来实现。包过滤路由器的最大优点是：对用户来说是透明的，即不需要用户名和密码来登陆。包过滤路由器的弊端是明显的，由于它通常没有用户的使用记录，我们不能从访问中发现黑客的攻击记录。它还有一个致命的弱点，就是不能在用户级别上进行过滤，即不能识别用户与防止 IP 地址的盗用。如果攻击者将自己的主机设置为一个合法主机的 IP 地址，则很容易地通过包过滤防火墙。

2.4.2 代理防火墙

代理防火墙也叫应用层网关防火墙，包过滤防火墙可以按照 IP

地址来禁止未授权者的访问。但它不适合单位用来控制内部人员访问外部网络，对于这样的企业，应用代理防火墙是更好的选择。

代理服务是设置在 Internet 防火墙网关上的应用，是在网管员允许下或拒绝的特定的应用程序或者特定服务，一般情况下可应用于特定的互联网服务，如超文本传输、远程文件传输等。同时还可应用于实施较强的数据流监控、过滤、记录和报告等功能。

2.4.3 复合型防火墙

复合型防火墙是将数据包过滤和代理服务结合在一起使用。从而实现了网络安全性、性能和透明度的优势互补。

总之，防火墙是网络安全的关口设备，安装防火墙的原则是：只要有恶意侵入的可能，无论是内部网还是外部网的连接处都应安装防火墙。计算机网络不安全因素的防治，单纯依靠技术手段是不可能十分有效地杜绝和防止其蔓延的，只有把技术手段和管理机制紧密结合起来，提高人们的防范意识，才有可能从根本上保护网络系统的安全运行。

参考文献：

[1] 郑成兴著.《网络入侵防范的理论与实践》机械工业出版社

[2] [美]MerikeKaeo 著.《网络安全性设计》人民邮电出版社

黑客攻防

微软下周发布 11 个安全补丁 修复 25 处漏洞

文章来源：中国物联网

下周二的例行补丁发布日微软将发布 11 个安全补丁，修复 25 处安全漏洞，涉及 Windows、Office 和 Exchange，其中修复的两个漏洞之前已经被曝光，攻击代码也被公布在网上。

在下周将发布的 11 个补丁中，有 5 个将修复高危级别漏洞，可导致远程代码攻击。此外的五个为重要级别，最后一个为中等级别。

此次发布的安全漏洞影响软件包括：Windows 2000、XP、Vista、Windows 7、Server 2003、Server 2008、Office XP、Office 2003、2007 Microsoft Office System 和 Exchange Server 2000、2003、2007 和 2010。

其中 KB981169 将修复 VBScript 中的一个安全漏洞，这个漏洞可导致系统遭受远程代码攻击。这个安全漏洞早在 3 月 1 日就被曝光，主要影响到运行 IE 浏览器的老版本 Windows。

下周微软还将修复一个早在去年 11 月份就被曝光的漏洞，该漏洞存在于 SMV 协议中，黑客可以利用该漏洞进行拒绝式服务攻击。

Sun Java 漏洞影响 Java SE 6 到 10 版本

文章来源：ZDNET 安全频道

最近一份安全报告上，Dennis Fisher 发现一个关于 Java 的严重安全漏洞，该漏洞能使用户开发 Windows 系统权限，使得简单的 Web 攻击就可以让黑客在用户电脑中为所欲为。

这个漏洞是由两位不同的研究人员在本周独立披露的。其中的一位，Google 的 Tavis Ormandy 表示，如果 Sun 不能迅速的发布漏洞解决补丁，他将公开漏洞的细节。

Ormandy 解释说：

Sun 已经通报了这个漏洞，但他们告诉我，他们不认为这个漏洞有较高的安全威胁优先级，他们不会打破每个季度发布补丁的周期性。

由于种种原因，我不认可这种做法，我将持续关注，指导这个问题至少有暂时性的解决方案。

另外一名独立发现者 Ruben Santamarta 发现这个漏洞的原因是因为包含 Java 插件的浏览器运行没有命令行参数的“Javaws.exe”。

Santamarta 警告说，这些参数可以被黑客利用于通过特定的控制嵌入网页的 HTML 代码。

Google 的 Ormandy 表示，这个工具提供了最小 URL 参数验证，这个错误可以被黑客利用，通过命令行参数，允许执行任意参数的 Javaws 程序。

Ormandy 认为，发布漏洞的细节可以帮助很多软件供应商来应对这个简单的错误。

这个漏洞影响到 Windows 中的 Java SE 6 到 10 版本，禁用 Java

插件不足以抵御这个危害，因为该软件是通过工具包形式单独安装。

Ormandy 建议用户进行如下操作来降低风险：

- Internet Explorer 用户应该保持他们的缓存设置在 CAFE EFAC - DEC7 - 0000 - 0000 - ABCDEFFEDCBA 终止位。根据他的了解，部署工作包没有得到广泛的部署，因此不会对终端用户造成大规模影响。

- Mozilla Firefox 以及其他的基于 NPAPI 的浏览器用户可以使用文件系统 ACL 防护，以防止黑客进入 npdeploytk.dll，这些 ACL 可以通过 GPO 来管理。

Facebook 农场被指含嵌恶意广告 导向假冒网站

文章来源：腾讯科技

4 月 13 日，据国外媒体报道，一位名叫 Sandi Hardmeier 的安全研究员日前发表博文称，Facebook 网站上的农场（Farm Town）应用中内嵌广告属恶意广告，它会将用户导向一些销售假冒杀毒软件的网站。农场是 Facebook 网站上的热门应用之一，据说每月用户在 900 万人以上。

Hardmeier 称，如果农场中内嵌的那个 Shockwave Flash 格式的广告被显示出来的话，用户就会被通过几个域名引导到一个销售假冒杀毒软件的网站。

农场的开发商 SlashKey 在其网站上发布了一则声明，声称公司已经将这个问题告知开发员。

SlashKey 在声明中表示：“我们相信这个问题不会危害到您的电脑，只会显示一些广告，但是如果有软件提示您‘清理您的系统’，请不要点击相关链接。大多数真正的杀毒软件都会检测出这个恶意链接。”

Hardmeier 对此持不同意见，她认为这个问题会危害到用户的电脑。她说：“我对 SlashKey 发布这样的声明感到失望，它想将隐含的观念降到最低。”

假冒杀毒软件网站通常会告知用户他们的电脑已经感染了病毒，然后要求用户下载一些软件，而那些软件通常都是完全无效的。那些软件的售价为 70 美元，而且很难清除。用户一旦支付了购买软件的费用，通常也很难再追回。

目前业内一共有数百种假冒杀毒软件，安全专家们估计这个市场的规模大概在数百万美元左右。安全公司熊猫安全 (Panda Security) 去年发布了一份研究报告称，每月全球大约有 3500 万台电脑被假冒杀毒软件感染。

据 Hardmeier 称，谷歌的 Chrome 浏览器可以检测出这个恶意广告引导用户所用的恶意域名并成功拦截攻击。谷歌在 Chrome 浏览器中内建了安全浏览 (safe browsing) 技术，可以阻止用户访问潜在恶意网站。然而，微软的 IE8 浏览器却做不到这一点。截至本文发稿

时, Hardmeier 正在测试火狐浏览器对这个问题的检测性能, 尚未得出最后的结论。

Hardmeier 称, 她已经通知了为农场提供广告的 cubics.com, 现在正在通知 Facebook。Facebook 官方尚未对此发表意见。

QQ 申诉系统疑存在严重漏洞

文章来源: 新浪科技

4 月 12 日晚间, 腾讯 QQ 出现大范围登陆异常, 有网友向新浪科技反映, 腾讯 QQ 的申诉系统疑似存在严重漏洞。根据这名网友的描述, 胡乱编写的申诉内容也可通过申诉, 而 QQ 帐号的安全因此面临威胁。

今日有网友张先生联系新浪科技, 称发现腾讯 QQ 申诉系统疑似存在严重漏洞。

事情的起因是, 4 月 10 日晚张先生发现自己的 5 位数字 QQ 帐号被盗, 并且 QQ 密码保护资料被篡改, 无奈之下, 张先生只能通过 QQ 申诉的方式取回密码, 并得以成功。但此事让张先生觉得非常蹊跷。

张先生为了验证 QQ 申诉系统的安全性, 又分别于 4 月 11 日晚, 4 月 12 日早晨, 分别再次进行申诉测试。在测试期间, 张先生提交的所有信息全部为临时随机敲打, 完全不符合逻辑的资料信息。

“比如历史密码我几乎是全部胡乱敲打键盘, 申诉人姓名也几乎正常人看到就不是一个人的姓名, 并且包括证件号码在内的所有信息,

完全虚构”，张先生说。

然而让张先生感到惊讶的是，腾讯申诉系统居然 2 次均通过了申诉，并且可以重新设置密码与保护资料。

就此问题，腾讯方面对新浪科技表示，QQ 号码的申诉系统为机器自动判别，就算所填写的资料异常，但核心资料是正确的一样可以通过申诉，为的就是避免用户记错所设置的信息。其中一条核心的判断标准是，所使用的邮箱是否相同。

不过，张先生在两次测试中使用了不同的电脑，并留下了不同的电子邮箱。

张先生表示自己“深感此事件异常重大，且关乎众多网民的切身利益”。由于腾讯方面表示 3 日内才能给予答复，张先生还是希望能引起更多网友重视，尽管“目前尚不知道是个人案例，还是普遍现象”。

好消息是，今晚八点张先生收到第三次测试的结果：申诉未予通过。至截稿时，腾讯方面也没有就此问题答复新浪科技。

由于象 Facebook 那样的热门社群网站拥有大量的用户和潜在受害者，因此它们是各种恶意网络攻击的主要目标。行过滤，网络管理员完全可以在攻击到达用户前将其阻断。对所有相关环节进行监测便可获得最有效的保护。”

Java 漏洞致 Windows 面临攻击危机

文章来源：hackbase

研究员警告，Java 技术有个安全漏洞，可能让黑客利用来发动攻击，入侵执行 Windows 操作系统的电脑，只要受害者造访内含恶意程序代码的网页，就能让黑客得逞。

Google 工程师 Tavis Ormandy 在 Full Disclosure 电子邮件论坛中有详细的描述，而同时 Wintercore 的工程师 Ruben Santamarta 也在公司博客上谈论此事。

问题出在 Java Web Start 架构，此架构让开发者轻易制作 Java 应用程序。若只是关闭这个 Java 外挂程序 (plug-in)，并不能防堵攻击。

Ormandy 写道：这个工具包 (toolkit) 只提供极有限的 URL 参数验证，以致能让任意的参数通过 javaws Java Web Start 公用程序，而后者借命令列参数 (command line arguments) 提供足够的功用，让黑客能利用这个错误。他还说：由于很容易就能发现这项错误，我相信，公布这个文件对大家都好，只有软件厂商除外。

根据 Kaspersky Lab 的 Threat Post 博客，上述安全漏洞影响所有目前的 Windows 版本，以及包括 Firefox、Internet Explorer 和 Chrome 在内的主要浏览器。

Ormandy 表示，他已向 Sun 通报这个问题，但对方告诉他，问题尚未严重到必须在每季例行安全更新日之前发布补丁程序的地步。

自学成才网络高手攻击金盾网

文章来源: hackbase

浙江台山男子做网络生意狂遭黑客攻击,阻挡无果后竟将攻击转到广州市公安局的金盾网,最终导致其被攻陷瘫痪……近日,他被警方抓获后,越秀区法院以破坏计算机信息系统罪对其提起公诉。

据查明,宋某是一名自学成才的网络高手,去年 3 月做起出租域名和网络空间的小生意。凭借其良好的技术服务,客户越来越多,每月能赚到一两万元。但随着生意越做越红火,一些黑客也盯上了他的服务器,不断向其服务器发起攻击,导致其服务器访问缓慢甚至完全瘫痪。无奈之下,去年 9 月宋某想到了一个“高招”,他通过修改 DNS 域名解析记录,将黑客的攻击行为转嫁到金盾网,造成金盾网无法访问。

金盾网的异常引起公安机关高度重视,立即通过技术手段对有关电子证据进行了保全,并顺藤摸瓜将远在浙江省台州市的宋某缉拿归案。令人啼笑皆非的是,宋某自称这么做只是想给公安机关提个醒,以引起有关部门对网络黑客攻击行为的重视,代其抓住幕后黑手。

黑客利用 Java Web Start 安全漏洞展开攻击

文章来源: 中国安全 作者: 文良

据国外媒体报道，互联网安全专家 4 月 14 日警告称，基于 Java 技术的应用程序解决方案 Java Web Start 中存在安全漏洞。目前已经发现黑客利用该漏洞攻击用户电脑，使用户直接链接到 Songlyrics.com 网站的行为，预计黑客将利用该漏洞对更多用户展开攻击。

捷克国内著名杀毒软件企业 AVG 公司首席研究院罗杰·汤普森称，Java Web Start 中的安全漏洞将对 Windows 操作系统下运行的火狐浏览器及 IE 浏览器造成潜在威胁。但就目前的研究结果表明，谷歌的 Chrome 浏览器不会造成安全威胁。

目前已经发现黑客利用这个 Java 安全漏洞，及俄罗斯境内的一个 Adobe Reader 服务器上的安全漏洞对全球电脑用户进行攻击，使用户浏览器直接链接访问 Songlyrics.com 网站。当用户访问一个托管恶意代码的网页后，即使用户没有点击网页上的广告，广告中带有的恶意 iFrame 插件将自动使用户浏览器链接托管服务器。其中，一种攻击会造成用户电脑在 window 操作系统下弹出 Adobe Reader 对话框，另一种攻击会使用户电脑链接到另外的服务器上抓取恶意 Java 文件。



国迈移动存储设备管理系统

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。

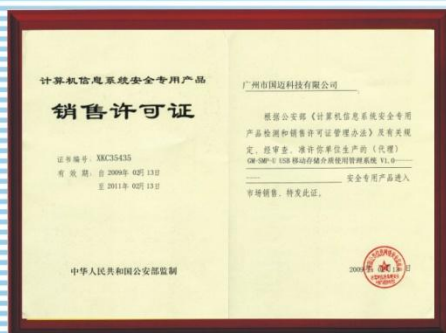
■ 六类专用安全U盘：

安全U盘、增强型安全U盘、单向导入U盘、单向导出U盘、双向交换U盘、外部受限使用U盘

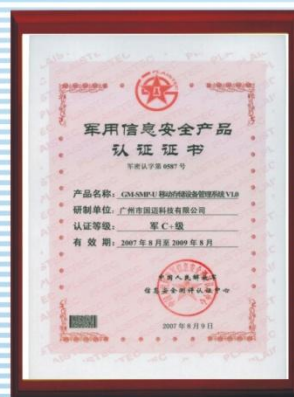
权威认证：



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、核工业某研究院、山东公安、广东公安、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