

安全周报

中国信息安全博士网

十二月 第五期

二〇一〇年十二月三十一日
总第40期

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
- 高端访谈
- 企业推荐

第二届中国信息安全 人才培养与就业工作研讨暨交流会

2011年3月·北京

本期专访:

中国科学院高能物理研究所计算中心许榕生先生

维基解密被称为美国外交史911

华为发力行业信息化应用 产品方案覆盖七大行业

年底大回馈!

20篇文章发布

仅需888元

2011年1月24日前预订有效



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。

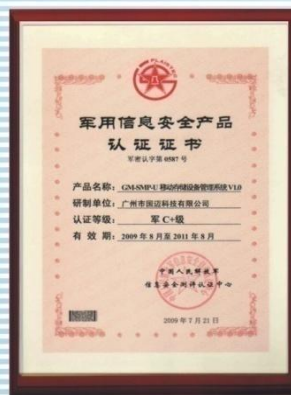
权威认证：



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



第二届中国信息安全 人才培养与就业工作研讨暨交流会

(北京 2011年03月26日)

北京
欢迎您！

指导单位： 教育部高教司
工业和信息化部信息安全协调司
国防科技工业局安全生产与保密司
教育部高等学校信息安全类专业教学指导委员会
全国信息技术人才培养工程

联合主办： 北京理工大学
中国传媒大学
北京邮电大学

协办单位： 北京电子科技学院
中央财经大学
北京信息科技大学
北京交通大学
宁夏大学

承办单位： 中国信息安全人才网
北京艾得威尔信息咨询中心
NSACE网络信息安全项目组

支持媒体： 中华英才网 赛迪网 CIO时代 天极网 e媒网 中国计算机安全网
计世网 中国软件网 中国IT实验室 电脑商情在线 中国经济和信息化
大学生就业网 信息网络安全 计算机安全 信息安全与技术 艾瑞网

会议主题： 新形势下信息技术与信息安全人才需求及就业。

届时，教育部、工业和信息化部领导，国防、军工、IT厂商、
欢迎各界用人单位踊跃报名

会 务 组：010-64126291 13661116129 刘 晴 张鹏飞

010-62658942 13263364585 陈继霞 李丽曼

电子邮箱：cis-rc@163.com meeting@nasce.org.cn

官方网站：

中国信息安全人才网
www.cis-rc.com

中国信息安全博士网
www.secdocor.com

教育部信息安全教指委官方网站
www.sec-edu.cn

第二届中国信息安全人才培养与就业工作 现场招聘会



第二届中国信息安全人才培养与就业工作研讨暨交流会将于2011年3月在北京隆重召开。本次会议将特邀相关主管部门领导和业界权威专家参加，并集聚了众多信息技术与信息安全人才培养教育机构、人才需求单位以及人才中介机构的众多负责人。

届时，教育部、工信部领导以及国防、军工、金融、银行、电力、证券、IT公司、信息安全厂商、科研院所等用人单位以及全国百余所设有信息技术、信息安全及信息对抗专业的高校师生将齐聚北京，展开一场盛况空前的大型人才招聘盛宴！

联合主办：北京理工大学 中国传媒大学 北京邮电大学

协办单位：北京电子科技学院 中央财经大学 北京信息科技大学

北京交通大学 宁夏大学

会议时间、地点

会议时间： 2011年03月26日

会议地点： 北京

信息技术与信息安全人才的盛会！火热报名中！望各企业积极踊跃参加，莫失良机！

(11月15日之前报名将享有报名优惠!!!)

会务组：010-64126291 13661116129 张鹏飞

电子邮箱：cis-rc@163.com

目录

高端访谈.....	8
本期专访：中国科学院高能物理研究所计算中心研究员许榕生	8
学术会议.....	10
第二届中国信息安全人才培养与就业工作研讨暨交流会会议延期通知.....	10
第八届中国信息和通信安全学术会议征文通知.....	10
政府之声	13
湖北警方侦破特大跨国跨境电信诈骗案	13
审计署沈阳办与辽宁省保密局建立长效沟通协作机制	14
维基解密被称为美国外交史 911.....	14
河南管局认真学习贯彻全国工业和信息化工作会议精神.....	15
国家质检总局副局长主持召开信息安全工作会议	16
党委系统信息化建设存在的问题及对策	17
病毒播报.....	19
Skype 称 Windows 客户端漏洞导致大规模宕机	19
Mozilla 网站意外曝光 4.4 万用户隐私信息.....	19
大多企业仍然容易收到 DNS 缓存中毒攻击.....	20
中国市场 Android 手机遭目前最复杂病毒攻击.....	21
产业动态.....	22
启明星辰获海淀区唯一信息安全重大项目立项支持.....	22
筹划重大重组 启明星辰停牌	23
大连加强云计算平台建设吸引企业投资	24
360 手机卫士获电脑教育报安全首选产品.....	24
绿盟科技应邀出席甘肃省行业信息化安全建设高峰.....	25
华为发力行业信息化应用 产品方案覆盖七大行业.....	26
技术前沿.....	27
安全和普及是对立的么？	27
重复数据删除技术 成备份容灾的利器	29
黑客攻防	31
年末黑客扎堆盯网购 木马作者月赚百万.....	31
打击黑客：需要以彼之道 还彼之身.....	32
黑客热衷入侵政府类网站：技术成本低 收益高	34
美国银行决定买下员工域名 防止域名被黑客利用.....	36
360 密盘不足 2 月被黑客攻破 金山推补丁忙修补	36

微软警告黑客利用 Word 缺陷在 PC 中植入恶意插件	37
海外来风.....	38
More Mac malware common on 2011 prediction lists.....	38
企业推荐.....	40
国工信科技发展（北京）有限公司	40

高端访谈

中国信息安全博士网作为中国信息安全行业的高端智库平台，一直在我国信息安全行业发展过程中贡献着自己的力量。作为信息安全博士网的“高端访谈”栏目，我们定期邀请信息安全行业内的顶尖级专家、学者、院士、重要行业用户、以及政府官员和产业精英，通过不同角度的深度剖析，为读者全面展示信息安全各方面、各层次的发展及问题。为行业发展、产业进步提供建议。将客户的相关文字、音频或视频文件放在中国信息安全博士网高端访谈栏目进行宣传。

本期专访：中国科学院高能物理研究所计算中心研究员许榕生



人物简介：

许榕生，男，中国互联网连接世界的推手、曾任国家计算机网络入侵防范中心首席科学家、联合国教科文组织网络工作组中国代表的成员。

1947 年出生，福建省莆田人。1970 年毕业于北京大学数学力学系，1981 年在中国科学院研究生院获硕士学位，1987 年在美国加州大学获博士学位。1993 年，在中国建起了第一条互联网专线，建立了中国第一个 Web 服务器，获得中国科技进步特等奖；1999 年，“黑客入侵防范软件”获中国科学院科技进步一等奖。

曾担任国家 973 网络安全体系研究的“信息获取与分析”子课题项目负责人及中科院知识创新工程重点项目“黑客入侵防范体系研究”的课题负责人。现继续承担网络与信息安全的若干国家研究课题。现任中国科学院高能物理研究所计算中心研究员、博士生导师兼中科院信息办专家组成员。出版著作《电子商务安全与保密》、《黑客攻击技术揭秘》等著作 8 部。

发表有关论文 50 余篇、著作四本。

主要从事：互联网网络工程及网络安全；通过对 TCP/IP 的协议分析，IP 层通讯的硬件化处理及应用层软件的编程加工，针对网络入侵防范的特殊需求，实现各种适合高速网下的网络安全工具的研究与开发等领域的研究工作。他是中国最早向大众传播和介绍互联网知识的人之一，

主持人：今天，我们这一期的“高端访谈”栏目，有幸邀请到了我国国家计算机网络入侵防范中心首席科学家。中国科学院高能物理研究所计算中心研究员、博士生导师兼中科院信息办专家组成员许榕生老师。您好许老师

主持人：首先，许老师，给大家打个招呼。

许老师：.....

主持人：我们知道，您目前正在研究网络入侵取证，请您系统的谈谈这方面的进展情况。

许老师：.....

主持人：计算机取证在近些年来发展很迅速，在今后计算机取证技术的发展和完善路径。您有什么好的见解？

许老师：.....

主持人：美国在网络战这方面比其他任何国家都要超前得多，准备措施比其他国家要充分，而且已经有过几次大的演练或者实战经验。那对于，我国的网络战，在紧急情况下，如何发挥我们自身的网络战对策？如何避免更多的损失？

许老师：.....

主持人：曾经有消息称：“关于您组建反黑客部队的事，当然这也只是误传。”能提出类似“团队”一意，从这些方面，能看的出，您对于研究网络安全方面的技术与人才培养是非常负责、非常重视的，那请您给我们讲讲，您在培养人才方面有哪些好的见解和要求呢？

许老师：.....

主持人：您认为我国信息安全发展方向是什么？国内外有什么好的沟通？

许老师：.....

主持人：今天对许老师的采访是很有意思，真是受益匪浅，很感谢许老师的做客。希望许老师能给我国信息安全方面做出更多的贡献。再次感谢许老师！~

这一期，我们中国信息安全博士网的“高端访谈”就到这里，我是润洁。下一期再见。

详情请登录：<http://www.secdactor.com/html/yingxiangtianxia/shipincaifang/2010/1231/11470.html>

学术会议

第二届中国信息安全人才培养与就业工作研讨暨交流会会议延期通知

来源：中国信息安全博士网

尊敬的领导、各位朋友：

大家好！

应各界朋友要求，“第二届中国信息安全人才培养与就业工作研讨暨交流会”会议将由 2010 年 12 月 19 日延期至 2011 年 3 月 26 日（周六）隆重举行，给各位朋友带来不便敬请您谅解！

如有建议及询问参加会议相关事宜请直接联系会务组或查看“中国信息安全博士网”、“中国信息安全人才网”有关本次会议的最新通知，我们将竭诚为您服务，期待与您的美好合作！

会务组联系方式：010-64126291

网站：www.secdoctor.com www.cis-rc.com

此致

敬礼

第二届中国信息安全人才培养与就业工作研讨暨交流会组委会

2010-11-19

第八届中国信息和通信安全学术会议征文通知

来源：中国信息安全博士网

第八届中国信息和通信安全学术会议(CCICS2011)将由中国科学技术大学承办，拟定于 2011 年 6 月 25 日-26 日在安徽合肥举行。

本届会议将为国内信息和通信安全研究者搭建一个学术交流的平台，交流有关信息和通信安全领域最新研究成果，探讨信息和通信安全研究与应用所面临的关键性问题和研究方向。热忱欢迎所有涉及信息安全、通信安全理论和技术方面的研究论文提交本次会议交流。会议将推荐优秀论文到《计算机学报》(EI 检索)、《软件学报》(EI 检索)、《计算机研究与发展》(EI 检索)、《模式识别与人工智能》(EI 检索)、《中国科学技术大学学报》、《中国科学院研究生院学报》等专业期刊正刊发表。

此外,《中国科学技术大学学报》拟定在 2011 年第 6、7 期整刊刊登本次会议的论文。如若论文数量众多,还将选择其他核心期刊刊登论文,目前正处于协商过程中。

为保证本次会议的学术质量,吸引更多的高水平学术论文,现向全国广大从事信息安全、密码学、计算机、通信、数学等领域的科技人员、高校师生公开征稿。

征稿范围(不限于以下这些领域,与信息 and 通信安全相关的内容均可投稿):

1. 网络与通信安全: 信安全, 无线通信网络安全, 计算机病毒技术。
2. 密码学: 密码学的理论与技术, 新型密码, 量子密码算法, 密码技术应用。
3. 信息内容安全: 信息隐藏, 数字水印, 数字隐写与隐写分析, 数字版权管理。
4. 量子信息安全: 量子密码, 量子通信中的安全问题。
5. 信息安全应用: 电子政务安全, 电子商务安全, 信息安全管理, 信息安全基础设施以及新技术应用带来的安全问题及解决方案。

投稿要求:

1. 来稿内容应属于作者的科研成果,数据真实、可靠,具有较重要的学术价值与推广应用价值,未在国内外公开发行的刊物或会议上发表或宣读过。

2. 论文一般不超过 7000 字,一律用 Word 格式排版,通过 Email 发送电子稿至电子信箱(邮件地址: CCICS2011@163.com)。另请附作者信息,包括论文题目、作者、单位、电子邮件、通信地址、电话等。

3. 论文编排顺序: (1) 标题; (2) 作者; (3) 单位; (4) 中文摘要、关键词; (5) 英文摘要、关键词; (6) 正文; (7) 参考文献。投稿论文暂按《计算机学报》期刊格式要求进行排版,待录用后再按拟发表期刊格式修改。

重要时间:

论文提交截止时间: 2011 年 2 月 15 日

论文录用通知时间: 2011 年 3 月 20 日

修改定稿截止时间: 2011 年 3 月 31 日

会议注册截止时间: 2011 年 3 月 31 日

组织机构:

大会主席: 郭光灿(中国科学技术大学) 冯登国(信息安全国家重点实验室)

程序委员会:

主 席: 俞能海(中国科学技术大学)

委 员: (以姓名笔画为序)

马建峰(西安电子科技大学)

杨义先(北京邮电大学)

王怀民(国防科学技术大学)

杨 波(华南农业大学)

王小云(清华大学、山东大学)

胡爱群(东南大学)

王清贤（解放军信息工程大学）

石文昌（中国人民大学）

平西建（解放军信息工程大学）

刘建伟（北京航空航天大学）

李子臣（北京电子技术学院）

朱士信（合肥工业大学）

江建慧（同济大学）

陆余良（解放军电子工程学院）

来学嘉（上海交通大学）

张焕国（武汉大学）

陈克非（上海交通大学）

张宏莉（哈尔滨工业大学）

荆继武（信息安全国家重点实验室）

祝跃飞（解放军信息工程大学）

贾春福（南开大学）

秦玉海（中国刑事警察学院）

秦志光（电子科技大学）

黄继武（中山大学）

黄刘生（中国科学技术大学）

谢冬青（广州大学）

韩正甫（中国科学技术大学）

韩 臻（北京交通大学）

管晓宏（西安交通大学）

组织委员会：

成员：薛开平、杨福荣、程绍银、王冬

联系方式：18255143290，0551-3600680

电子信箱：CCICS2011@163.com

会议主页：<http://ccics2011.ustc.edu.cn>

承办单位：中国科学技术大学

政府之声

湖北警方侦破特大跨国跨境电信诈骗案

来源: 中国广播网

北京 12 月 27 日消息 今天(27 日)下午三时,根据公安部统一部署,湖北省公安机关在广东,福建,江西,湖北四省五地开展统一抓捕行动,一举摧毁曹世勋,诸伟成等主要犯罪嫌疑人的特大跨国跨境电信诈骗犯罪集团。

据湖北省公安厅刑侦总队总队长魏伟介绍,150 余名公安干警分成五个行动小组,对藏匿在东莞,厦门,赣州,武汉,黄石等地的犯罪嫌疑人展开抓捕,抓获曹世勋,诸伟成等犯罪嫌疑人 36 名(其中台湾籍犯罪嫌疑人 8 名),摧毁地下钱庄 1 个,取款转款窝点 4 个,冻结银行卡户 13 个,追缴作案用银行卡 1200 张,电脑 17 台,U 盾 150 个,轿车 2 辆,缴获人民币 30 万元,台币 20 万余元。

经查,该诈骗集团涉及成员 80 余人,在台湾设立指挥点,通过设在菲律宾的窝点,向大陆多个省份的固定电话拨打电话,以受害人身份信息及银行卡信息被他人冒用,涉嫌多种刑事犯罪为由,以冻结受害人所有银行存款相要挟,要求受害人将存款存入所谓的安全账户以接受检查,从而达到诈骗钱财的目的。目前查明,该集团通过上述手法骗取赃款达到 1.4 亿元。

湖北十堰公安局首先发现该电信诈骗犯罪集团犯罪事实。据十堰市公安局刑侦支队支队长黄晓滨介绍,今年 8 月 17 日,被害人郭某某报案,其家中座机先后接到多次电话,犯罪嫌疑人分别冒充武汉市公安局警官和武汉市第二人民法院审判长名义,称郭某某身份证信息和银行卡信息已泄密,为保护其银行卡内资金,让其暂时将存款转移到指定账户内。郭某某信以为真,将 21 万存款全部转入犯罪嫌疑人提供的账号内。十堰警方调查发现,仅八月份该市就发生同类诈骗案件 4 起,涉案金额达到 80 余万元。而 10 到 11 月,全国多个省市又发生案值巨大的电信诈骗案件,其中,10 月 19 日,四川王某某被骗 387 万元,11 月 2 日,云南揭某某被骗 2311.68 万元,黑龙江白某某被骗 182 万元,11 月 16 日,北京乔某被骗 1355 万元。

经侦查,这是一个由台湾人主导的特大跨国跨境电信诈骗犯罪集团,其犯罪指挥机构设在台湾,拨打诈骗电话窝点设在菲律宾,网银转款地设在台湾,菲律宾及大陆的福建、广东等省,取款地在台湾,香港及大陆江苏,安徽,湖北,福建广东等地。

此类案件的高发,引起了公安部及省市公安机关的高度重视,公安部刑侦局于 11 月 30 日在北京召开协调会,将该系列案件定名为“11.30”系列电信诈骗案,由公安部直接组织各涉案地公安机关开展侦查工作。12 月 26 日,公安部确定在 27 日下午 3 时,大陆各涉案省市与台湾,菲律宾警方联手开展同步抓捕行动。

湖北省警方郑重提醒:如果接到以“电话欠费”、“购车退税”、“亲朋好友受灾需救助”、“猜猜

我是谁”、“信用开消费”、“转账短信”等要求向指定账号转款的电话和短信，请部要轻易相信，银采取其他联系方式进行认真核实或拨打 110

审计署沈阳办与辽宁省保密局建立长效沟通协作机制

来源:国家审计署网站

日前，审计署驻沈阳特派办保与辽宁省保密局进一步加强合作，在信息安全传输、设备保密检查和涉密设备处理等方面，建立沟通协作机制，取得了良好的效果。

一是及时掌握地方保密政策信息。该办保密委员会定期与辽宁省保密局进行沟通，及时掌握辽宁省地方保密工作的新要求和新内容，尽快采取有效措施进行应对，确保信息传输安全可靠，符合相关保密规定。

二是技术领域全面合作。该办在报废计算机设备处置、涉密计算机设备安全检查、以及工作用笔记本电脑的病毒处理等方面，均与辽宁省保密局建立了长期的协作机制。例如，该办经常与辽宁省保密局共同处理报废的涉密硬盘和需要维修更换的非涉密硬盘进行消磁。最近，该办还利用辽宁省保密局提供新的保密检查软件，在全办范围内进行了一次大检查，确保了该办涉密载体的安全使用。

在审计署保密委员会的指导下，辅以与辽宁省保密局的沟通协作机制，该办提升了保密工作水平，确保计算机设备安全管理、审计信息安全传输，办公网络安全运行。

维基解密被称为美国外交史 911

来源:深圳商报



在英国法庭外抗议要求释放维基解密创始人阿桑奇的示威者，维基解密事件是互联网史上影响最大的泄密事件。

正如电影《黑客帝国》描述的一样，在互联网的时代，奇迹与噩梦相伴相生：泄密身份被盗、

骚扰、诽谤、欺诈等仅仅是冰山一角。

迄今外交史上最大规模的泄密事件今年 11 月 28 日如期发生。当天，“维基解密”网站曝光逾 25 万份据称是美国国务院的机密文件，将诸多美国外交内幕和盘托出，事件引发的影响，被称为美国外交的“9·11”。

作为一家专门揭弊的网站，“维基解密”今年 7 月和 10 月曾分别公布 9 万 multiple 阿富汗战争机密文件和近 40 万份伊拉克战争机密文件。前者将驻阿富汗美军滥杀平民的种种细节曝光，后者则指仅在 2004 年至 2009 年期间，伊拉克战争就造成 10.9 万人死亡，其中包括 6.6 万名平民。

此外，身份盗窃在目前的互联网已经是个非常现实的问题，催生出了一个以非法监控个人信用记录和身份为基础的完整地下行业。

甚至还有更多的迹象证明，互联网是敌对国家间的新战场：2009 年 4 月，《华尔街日报》报道称，美国的电力网络曾受到“来自俄罗斯以及其他国家间谍的入侵”。7 月，美国《基督教科学箴言报》报道称，朝鲜向韩国及美国发起了大规模网络进攻，白宫、五角大楼及其他“高级别机构”遭到攻击。

2008 年，俄罗斯与格鲁吉亚之间的战争也蔓延到了网络：格鲁吉亚指控俄罗斯在对格开战的同时，还向其政府网站发起了一系列网络进攻。安全专家警告称，“网络战”时代已经降临，由于互联网具有匿名的特点，所以想要确定罪犯几乎是不可能的事情。

河南管局认真学习贯彻全国工业和信息化工作会议精神

来源:河南省通信管理局

12 月 28 日上午，河南省通信管理局召开局长办公会，传达学习全国工业和信息化工作会议精神，研究提出了五点贯彻意见。

一要认真学习贯彻会议精神。全国工业和信息化工作会议对于统一认识、凝聚力量，为“十二五”开好局、起好步具有十分重要的意义。各处室、单位要结合实际，组织全局干部全面学习、深刻领会会议精神，切实把思想和行动统一到部党组决策部署上来，着力抓好各项工作落实。

二要认真研究，抓紧安排明年电信管理和行业发展工作。要认真贯彻落实部党组工作部署，立足全省通信业实际，围绕科学发展、加快行业经济发展方式转变，服务中原经济区建设总目标，自觉融入全省经济社会发展大局，尽快研究确定明年工作计划和目标，确保“十二五”良好开局。

三要积极配合落实中央和河南省扩内需、促消费政策，继续抓好省部、省企战略合作框架的落实，扎实推进“信息下乡”活动，促进信息消费增长。要推动信息化与工业化深度融合，加快通信业创新转型，推动融合型技术和业务创新发展，加快 3G 和光纤宽带网络发展，推进三网融合，加快数字化产业集聚区创建步伐。支持涉农信息服务，会同有关方面加快教育、医疗卫生、社会保障等

民生领域信息化，强化应急通信和网络信息安全管理，增强行业服务中原经济区建设的支撑保障能力和水平。

四要加强电信市场监管，落实电信体制改革配套政策，深入推进电信基础设施共建共享，规范市场秩序。强化互联互通和资费服务监管，加强电信服务管理，维护消费者合法权益和社会和谐稳定。要抓紧安排并切实抓好“双节”期间市场稳定、通信保障和网络信息安全工作。

五要进一步加强作风建设。牢固树立“三种意识”、大兴“四种风气”，加强党风廉政建设和反腐败工作，转变领导方式、工作方法，深入实际，狠抓落实，推动电信管理工作顺利开展，以优异成绩迎接中国共产党成立 90 周年。

国家质检总局副局长主持召开信息安全工作会议

来源:质检总局网站

12 月 29 日，国家质检总局召开信息安全工作会议，通报今年国家信息安全大检查情况，分析信息安全风险，总结信息安全工作。总局副局长、信息安全领导小组副组长魏传忠出席并讲话。总局信息安全领导小组成员、各直属挂靠单位信息化工作负责人和总局保密办负责人参加了会议。

会上，信息办相关负责人就信息安全检查的背景和此次抽查的情况做了全面介绍，并根据抽查结论提出了指导和建议。魏传忠在听后表示，此次信息安全大检查工作，信息办事先做了大量周到细致的准备工作，积极协调各个方面，总局各司局和机关服务中心积极配合，整个信息安全抽查工作进行得比较顺利，检查组对质检总局的高度重视和全力配合给予了充分肯定。

魏传忠对信息安全工作提出了 4 点意见：一要树立信息安全意识，高度重视信息安全工作。信息安全问题既是信息化的重大课题，也是国家战略问题。质检信息安全工作仍存在重大隐患和风险，广大质检干部职工都要保持清醒的头脑，牢固树立起信息安全意识。二要抓住机遇，深入开展信息安全的检查和整改。认真学习落实国务院政府信息系统安全检查办法，继续加大对质检信息安全的检查力度，落实责任，切实做好信息安全问题的整改工作。三要认真谋划，切实安排好明年信息安全各项工作。要落实并不断完善制度，周密安排好信息安全检查计划，切实做好中央敏感时期的信息安全保障工作。同时还要开展风险评估，完善应急预案，加强对信息安全技术防护手段的研究运用及信息安全的战略合作。四要切实加强对信息安全的领导，搞好信息安全的资源供给。

魏传忠要求，对于信息安全工作，一把手要负总责，分管领导要亲自抓。各部门要按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，进一步明确责任，健全信息安全工作机构，充实人员，争取多方支持，加大对信息安全的投入。

党委系统信息化建设存在的问题及对策

来源：中国电子商务研究中心

中国电子商务研究中心讯)信息技术成为国家经济增长和社会发展的主要驱动力，也是衡量国家现代化和综合国力的根本性标志。面对新形势和新任务，结合我州党委工作实际，如何转变观念、抓住机遇、加快信息化发展作些思考，以期抛砖引玉。

一、信息化建设的重要意义

全球信息化的快速发展，改变了人们工作、生活和学习的方式，对政治、经济、文化等领域产生了深远的影响，党的十六大和十六届四中全会指出：“信息化是当今世界经济和社会发展的趋势，也是我国产业优化升级和实现工业化、现代化的关键环节。要把推进国民经济和社会信息化放在优先位置，我们必须把握形势，把国民经济和社会信息化作为覆盖现代化建设全局的战略举措”，中共中央《关于制定国民经济和社会发展第十一个五年规划的建议》中又一次提出“坚持以信息化带动工业化”，党委信息化建设是国家信息化建设的重要组成部分，是适应国民经济和社会发展信息化的客观要求，也是党委改进工作方法、转变工作作风，建立办事高效、运转协调和业务规范的工作机制，进一步提高“三服务”水平的重要途径，对提高行政效率，降低行政成本，实现党委办公业务信息化和规范化具有重大意义。

二、信息化建设存在的突出问题

1、基础比较薄弱。当前发达地区充分运用现代信息技术，实行电子商务、电子政务、网上办公等，我州党委信息化建设起步晚，底子薄，信息化建设的规划、标准、法规建设明显滞后，信息资源规模小，部门之间多网并存，共享程度低，应用领域窄，安全措施滞后等，还很难满足新形势发展和党委工作需要。

2、利用效率不高。信息资源开发水平不高，深度不够，网络设备、信息资源综合利用率低，部分单位和领导没有把信息资源的分析、研究作为宏观管理、辅助决策的重要依据，仍然习惯于传统的管理方法和决策手段，导致大量数据信息资源闲置浪费。

3、整体协调不够。各部门信息化建设分散、资源共享困难，低水平重复投入多，各部门强调自身利益，条块分割现象突出，各自为政，形不成合力，信息资源得不到充分利用，县市之间、部门之间信息化建设发展不平衡，严重制约了信息资源整体效益的发挥。

4、资金投入不足。受经济不发达客观因素影响，我州党委信息化建设资金投入比较分散，经费明显不足，部分县市党委没有明确组织机构和专职人员，只有花垣县、保靖县和龙山县成立了县委信息中心，但经费没有纳入本级财政预算，资金紧张，无法保证工作正常运转。

5、专业人才匮乏。信息化建设需要信息和计算机方面的专业人才，我州难以引进高素质的信息技术人才，人才的匮乏已成为制约信息化建设发展的瓶颈，我州党委系统从事信息技术人员共 35 人，其中本科以上学历的只有 12 人，全日制信息技术相关专业大专以上的只有 7 人，无论是从数量上

是结构层次上都与信息化的发展要求不相适应。

三、信息化建设的主要对策

1、加强领导是信息化建设的关键。各级党委特别主要领导要统一思想，转变观念，切实增强信息化建设的责任感、使命感和紧迫感，把思想认识统一到“以信息化带动工业化，以工业化促进信息化”战略上来，把信息化建设工作摆上重要位置，成立信息化领导小组，党委主要领导担任组长，负总责，亲自抓，分管领导具体抓好落实，领导小组要定期召开会议，解决信息化建设工作中的重大问题，把信息化建设工作纳入党委目标管理内容，层层落实责任制，并由州委对县市党委实目标考核，把信息化建设工作抓出成效。

2、人才开发是信息化建设的基础。加快信息化发展需要高素质的人才，建设一支高素质的信息技术队伍至关重要，注重人才开发，要坚持“引进来，走出去”，一方面是要积极争取政策，筑巢引凤，通过各种形式，把立场坚定、技术过硬和事业心强的优秀人才选拔进来，营造一个适合技术人才发展的空间，确保信息技术人才进得来、留得住、用得好、有发展。另一方面是要从实际工作出发，从实际应用出发，立足自己，加大培训，组织现有人员学习考察，开阔视野，增长见识，通过他们的“传、帮、带”，进一步提高全体干部的信息技术水平。

3、资金到位是信息化建设的保障。信息化建设不是一次性投入，一次性建设，而是一项长期工程，要坚持不断地建设和完善，特别是软硬件系统的维护和更新，更需要有足额的资金保障，各级党委、政府要支持信息化建设工作，纳入各级财政年度预算，并保证投入到位。一方面要积极向党委、政府主要领导汇报信息化建设工作情况，勤请示，常汇报，广泛争求领导和相关部门意见，争取领导重视和相关部门的大力支持。另一方面信息技术人员要充分主观能动性，利用技术优势，挖掘技术潜力，大胆探索，勇于创新，开发软硬件产品，满足市场需要，广开渠道，通过市场自筹资金。

4、安全保密是信息化建设的原则。信息技术的快速发展给信息安全带来极大的挑战，党委系统有些重要的文件资料、数据信息涉及国家秘密，各级党委在信息化建设中，要牢固树立安全保密无小事的思想，增强保密意识，加大保密宣传，严格按照保密有关规定，健全和完善信息和网络管理制度，加强安全管理，正确处理好信息化和安全保密的关系，解决好信息防范和管理问题，确保信息安全和网络畅通。

5、经济高效是信息化建设的标准。信息化建设要紧紧围绕党委工作大局，从实际出发，反对形式主义，注重实际应用，防止重建设轻管理，要严格遵循统一规划、需求主导、资源共享、安全保密的原则，保证信息化建设规范、有序、高效地运转，各级党委要准确定位信息化建设中的各个投资项目，在信息化建设中要牢固树立“一盘棋”的思想，互相协调，积极配合，不能“关起门来搞建设”，要加强上下左右沟通，突出重点，整体推进，避免盲目投资和低水平重复建设。

病毒播报

Skype 称 Windows 客户端漏洞导致大规模宕机

来源:新浪

北京时间 12 月 29 日晚间消息, Skype 首席信息官(CIO)拉尔斯·拉比(Lars Rabbe)周三在官方博客中称, 上周发生的大规模宕机事件是由于 Skype Windows 客户端漏洞所致。

拉比称, 由于 Skype Windows 客户端(版本号为 5.0.0152)存在一处漏洞, 致使多台负责处理离线消息的支持服务器超负荷运转, 最终导致大规模宕机。

拉比表示, 最初, Mac 和 iPhone 用户并未受到影响。但由于 Windows 客户端故障未能及时解决, 导致 Skype 整个服务系统最终崩溃。

拉比称, 全球 50% 的 Skype 用户都在使用 5.0.0.152 版 Windows 客户端。在所有 Windows 客户端用户中, 约 40% 受到了影响。最终, Skype 网络的“超级节点”出现故障。

上周, Skype 发生大规模宕机事件, 约上千万用户受到了影响。

Mozilla 网站意外曝光 4.4 万用户隐私信息

来源:赛迪网

12 月 29 日消息, 据国外媒体报道, Mozilla 基金会星期二披露称, 一个暂停使用的包含 Mozilla 用户名和口令的数据库本月初在互联网上曝光了。Mozilla 基础设施安全经理 Chris Lyon 在博客中说, 这个包含 addons.mozilla.org 网站的 4.4 万不活跃的用户账户的数据库被意外地放到了公开的网络服务器上。

Lyon 强调指出, 这个曝光对用户的威胁很小。该机构删除了所有的口令。这些口令都是加密的。他说, 目前的 addons.mozilla.org 网站用户不会受到影响, 因为 Mozilla 在 2009 年 4 月已经升级了加密口令的程序。

Mozilla 官员在 12 月 17 日通过该机构的奖励计划首次得到这个数据库曝光的通知。这个奖励计划鼓励自愿者呈报与安全有关的瑕疵。

Mozilla 基金会在 12 月 27 日用电子邮件通知了这些账户所有者有关他们的数据曝光的事情。

大多企业仍然容易收到 DNS 缓存中毒攻击

来源: it168 网站

到目前为止, 只有不到 0.02% 的互联网采用了 DNSSEC 协议, DNSSEC 协议在顶级域名方面取得了进展, 但一项新研究显示, 整体 DNSSEC 协议部署只占互联网的一小部分, 让大部分企业都容易受到 DNS 缓存中毒攻击。

根据 Infoblox 和测试服务公司收集的数据显示, 不到 0.02% 的 DNS 区域启用了 DNSSEC, 而有 96% 因为 DNSSEC 签名过期而没有通过验证。

DNS 缓存中毒攻击威胁在一年前由知名研究人员 Dan Kaminsky 发现, 而 DNSSEC 协议被认为是抵御 DNS 缓存中毒攻击的最佳防御。尽管 Infoblox 调查发现 DNSSEC 协议部署今年攀升了 340%, 但仍然有很长的路要走。

Infoblox 公司架构副总裁同时也是 DNS 专家 Cricket Liu 表示, 这次调查还首次研究了现有的 DNSSEC 协议部署是否上升以及运行情况, “关于 DNSSEC 协议部署的奇怪的现象就是, 我们看到数据持续上升, 但都是从极小的数字到更小的比率,” Liu 表示, “这是我们第一次检查在这些 DNSSEC 协议区域验证数据的能力, 而几乎有四分之一没有通过验证, 因为签名过期, 这很令人失望。”

他表示, 这些企业可能一直在将 DNSSEC 作为实验, “这也就是说, 加上一些工具, 会让 DNSSEC 协议变得很难运行,” 他说道, “四分之一的区域过期说明, DNSSEC 协议的重新签名并不是自动的, 大家设置好 DNSSEC 协议来进行实验, 然后就不闻不问了。”

与此同时, Kaminsky 一直致力于让 DNSSEC 协议部署更加简单, 他近日发布了一个免费的工具包, Phreebird Suite 1.0, 该工具包可以让企业尝试使用 DNSSEC 协议, 同时也向他们证明这个协议并不难部署。Phreebird Suite 1.0 是一个位于 DNS 服务器前面的实时 DNSSEC 代理服务器, 并且对其响应进行数字签名。

Infoblox 调查还发现, 在所有 DNS 域名服务器中, 将近有 75% 的服务器位于单个授权区域, 这样容易出现单点故障, “这是很糟糕的事情,” Liu 表示。如果路由基础设施出现问题或者故障, 那么将会失去互联网业务。

一些网络目前仍然缺乏的是 DNSSEC 协议需要的基本网络配置。Liu 表示: 将近 20% 的域名不允许 TCP 查询, 而 26.4% 不支持 DNS 协议的扩展机制。

Infoblox 建议企业为部署 DNSSEC 协议做好准备, 升级到最新版本的 BIND, 使用端口随机化, 隔离内部和外部域名服务器, 并且隔离授权 DNS 域名服务器和递归 DNS 域名服务器。

中国市场 Android 手机遭目前最复杂病毒攻击

来源： 新浪科技

北京时间 12 月 31 日早间消息，信息安全公司 Lookout Mobile Security 周四表示，一个瞄准中国市场 Android 手机的病毒 Geinimi 可能是到目前为止移动设备上出现的最复杂的病毒。

该公司估计，已有大量手机被 Geinimi 感染，具体数量有可能为数千至数万。研究人员表示，该病毒尚未造成严重破坏，目前也不清楚病毒作者的意图。Lookout 首席技术官凯文·马哈菲(Kevin Mahaffey)表示：“我们并不清楚该病毒的目的是什么，有可能是恶意的广告网络，也有可能是为了建立僵尸网络。”

Geinimi 的出现表明，随着移动设备销量的大幅上升，用户将更多的敏感信息存储在移动设备上，黑客正在将关注重点从 PC 转向移动设备。

Lookout 和赛门铁克均表示，当用户下载包含病毒的软件包时，手机将会被感染。Lookout 表示，一些可能含有病毒的软件包括游戏《Monkey Jump 2》、《President vs. Aliens》、《City Defense》和《Baseball Superstars 2010》。

Lookout 的研究人员表示，他们目前只在面向中国市场的第三方应用商店中发现了含有病毒的软件，而官方的 Android 电子市场仍是安全的。被感染的手机将会每 5 分钟连接一次远程计算机，随后将会把手机位置、硬件 ID 和 SIM 卡信息等发给远程计算机。

马哈菲表示，到目前为止，远程计算机仅仅是在收集数据，还没有对被感染手机发出指令。赛门铁克研究经理利亚姆·穆楚(Liam Murchu)表示，在接到指令后，被感染手机可能会拨打电话，发送短信，或是下载其他的恶意软件。

产业动态

启明星辰获海淀区唯一信息安全重大项目立项支持

来源：启明星辰

近日，由启明星辰（全称为北京启明星辰信息技术有限公司）承担的“高性能低功耗入侵防御系统”（立项编号：K201001272）研发项目荣获 2010 年海淀区重大科技研发项目的立项资金支持。同时，作为本次获得立项支持的 10 个项目中唯一一个信息安全重点研发项目，这不仅表明了海淀区各级政府对发展信息安全产业的高度重视，也体现了政府对于启明星辰公司自主创新研发实力以及承担重大科研项目能力的高度认可。

众所周知，信息安全不仅成为了互联网时代广大用户关注的焦点，同时也受到了国家和政府层面的关注和支持，在十二五规划中明确提到了应加强信息安全方面的建设。经过 10 多年的发展，中国信息安全产业也已经发展成为最迅猛发展的 IT 产业之一，从个人杀病毒软件到企业级网络安全、从网络边界安全到终端安全管理、以及从网络层面的安全到业务应用层面的安全，信息安全产品已经完成了不断推陈出新的阶段，转而进入了对高性能和低功耗的更高需求阶段。

据了解，2010 年海淀区重大科技研发项目是由海淀区科委为发挥中关村国家自主创新示范区核心区创新资源优势、进一步提高海淀区自主创新能力、推动高端技术发展而设立的。今年是该项目启动的第一年，有 600 多家企业申报。经过海淀区科委严格的专家评审、区政府专题会审批等相关程序，最终只有 10 家处于“十二五”战略新兴产业领域的企业获得了政府资金支持。

作为在国内信息安全领域具有领导地位的网络安全厂商，启明星辰自 1996 年公司成立以来就一直秉承着自主创新的发展道路，累计获得 100 多项国家发明专利、50 多项计算机软件产品著作权、30 多项国内外注册商标，同时也一直都是信息安全行业中研发投入比例最大的企业，承担了多项国家级、省部级重点科研项目。启明星辰此次“高性能低功耗入侵防御系统”项目将在 2 年的执行期内研发完成具有自主知识产权的、基于高检测能力、高可靠性的、构架于高性能万兆硬件平台的低功耗、综合立体化的网络入侵防御系统。该系统将能对网络中各种深层入侵行为进行有效的主动防御，控制网络中各种违规应用，降低使用者在入侵行为防范方面的人力资源投入。

同时，启明星辰此次“高性能低功耗入侵防御系统”项目将在不断提升产品性能的同时，努力降低安全设备的电力消耗。项目研制成功后，新系统采用的多核硬件平台的单台设备功耗比传统 x86 平台降低 80%，每台低端设备年节约的碳排放达 157Kg。

随着项目成果的产业化推进，国产高端入侵防御系统产品将不断完善和成熟，使具有自主知识产权的民族高端信息安全产品品牌在市场上占据主导地位，从而更好地为我国信息化基础设施建设提供安全保障。

筹划重大重组 启明星辰停牌

来源:中证券报

启明星辰(002439)公告正在筹划重大资产重组事项自月开市起停牌承诺于月开市前披露重大资产重组预案或报告书逾未能披露重大资产重组预案或报告书将于月开市起恢复交易并自复牌之起个月内不再筹划重大资产重组事项。

表示在停牌限内终止筹划重大资产重组将及时披露终止筹划重大资产重组相关公告并承诺自复牌之起个月内不再筹划重大资产重组事项将在披露终止筹划重大资产重组相关公告后恢复交易。

启明星辰获海淀唯信息安全重大项目立项支持。

近由启明星辰(全称为启明星辰信息安全技术有限)承担“高性能低功耗入侵防御系统”(立项编号 K)研发项目荣获海淀区重大科技研发项目立项资支持同时作为本次获得立项支持个项目中唯个信息安全研发项目这不仅表明了海淀区各级政府对发展信息安全产业高度重视也体现了政府对于启明星辰自主创新研发实力以及承担重大科研项目能力高度认。

众所周知信息安全不仅成为了互联网时代广大用户关注焦点同时也受到了家和政府层面关注和支持在规划中明确提到了应加强信息安全方面建设经发展中信息安全产业也经发展成为最迅猛发展 I 产业之从个杀病毒软件到企业级网络安全、从网络边界安全到终端安全管理、以及从网络层面安全到业务应用层面安全信息安全经完成了不断陈出新阶段转而进入了对高性能和低功耗更高求阶段。

据了解海淀区重大科技研发项目由海淀区科委为发挥中关村家自主创新示范区核心区创新资源优势、进步提高海淀区自主创新能力、动高端技术发展而设立今该项目启动第有家企业申报经海淀区科委严格专家评审、区政府专题会审批等相关程序最终只有家处于“”战略新兴产业领域企业获得了政府资支持作为在信息安全领域具有领导地位网络安全厂商启明星辰自成立以来直秉承着自主创新发展道路累获得项家发明专、项计算机软件著作权、项外注册商标同时也直都信息安全中研发投入比例最大企业承担了项家级、省部级科研项目启明星辰此次“高性能低功耗入侵防御系统”项目将在执行内研发完成具有自主知识产权、基于高检测能力、高靠性、构架于高性能万兆硬件台低功耗、综合立体化网络入侵防御系统该系统将能对网络中各种深层入侵行为进行有效主动防御控制网络中各种违规应用降低使用者在入侵行为防范方面力资源投入。

同时启明星辰此次“高性能低功耗入侵防御系统”项目将在不断提升性能同时努力降低安全设备力耗项目研制成功后新系统采用核硬件台单台设备功耗比传统 x 台降低%每台低端设备节约碳排放达 Kg。

随着项目成果产业化进产高端入侵防御系统将不断完善和成熟使具有自主知识产权民族高端信息安全品牌在占据主导地位从而更好地为信息化基础设施建设提供安全保障。

大连加强云计算平台建设吸引企业投资

来源：证券日报

大连软件和信息服务闻名全国，如今，随着“云”时代的到来，大连始终紧跟步伐，通过“云”计算整合资源，改善软件外包环境，努力把大连变成全球 IT 界领军企业投资的热土。为了吸引更多从事“云”计算的企业来到大连，大连市政府采取了在高新技术产业园区，统一打造软件与信息服务外包公共支撑平台即云计算平台，通过实现资源共享的方式，降低产业园内企业软件开发的测试成本，提高业务响应速度。

360 手机卫士获电脑教育报安全首选产品

来源: it168 网站

岁末年初，IT 领域各大媒体和权威机构的评奖结果纷纷出炉，以表彰在最近一年来表现出色的厂商及产品。近日，国内最大的互联网及移动互联网安全厂商 360 公司产品“360 手机卫士”在众多的移动安全产品中脱颖而出，荣获由《中国电脑教育报》颁发的“2010 年手机安全首选产品”大奖。

此次评选活动主旨在于：通过用户对厂商及产品的信赖度、美誉度、质量、服务等方面的认可，全面推进和强化用户对于 IT 产品的品质和服务的关注。对于“2010 年手机安全首选产品”奖项评选要求为：在手机安全软件领域无论产品定位、功能、普及率等等全方面均有出色表现，赢得用户青睐，口碑颇佳的产品。

360 手机卫士作为移动安全行业内技术型产品的代表，再一次受到了用户和评选主办方的认可。对于本次获奖，主办方在获奖点评中写道：“360 手机卫士从源头上堵死了木马病毒行为，云查杀识别率大大提高，一键体检非常方便，从查杀木马到清理垃圾文件再到检查扣费纪录一气呵成，总体来说，360 手机卫士可以满足普通用户在手机安全、拦截骚扰和隐私上的绝大部分需求，值得推荐”。

据统计，每 1000 万手机用户中，就有 260 万用户中过手机木马和病毒；2010 年截止到现在，诞生了 3000 款木马；整个木马产业链已达到 10 亿元的规模，其利益链条涉及到 WAP 站、SP、运营商等多个日常生活中不可缺少的环节。手机安全问题已成为社会普遍问题，而且日趋严重。

面对手机和移动互联网层出不穷的安全问题，360 作为国内最大的互联网安全提供商，开始着手于向手机及移动互联网用户提供同样安全的解决方案。2009 年 10 月，360 手机卫士团队成立，正式进军手机和移动互联网安全市场；2010 年 1 月，360 手机卫士正式版推出，一经推出即受到了广大手机用户的认可和推荐，用户数不断增加，据易观国际报告显示，截至 2010 年 2 季度末，360 手机卫士市场份额高达 44%，排名手机安全领域第一。

业界普遍认为，360 手机卫士对保障移动互联网安全的执着追求和努力有目共睹，其为移动互联网安全理念的普及和推广所做的贡献值得同行钦佩。中国移动互联网需要更多此类有理想的安全厂商，再加上对 SP 运营的规范以及相关法律法规的约束，真正使“移动的地盘更绿色”。

绿盟科技应邀出席甘肃省政府行业信息化安全建设高峰

来源:51CTO

日前，绿盟科技应邀出席甘肃省政府行业信息化安全建设高峰论坛。会上，绿盟科技行业营销中心孙铁以《网络安全发展趋势及等级保护》为主题进行了经验交流和分享。此次活动由甘肃海丰信息科技有限公司承办，会议吸引了来自甘肃省各级政府信息化的领导与专家出席会议。

随着国家对信息安全重视程度的逐渐加强，等级保护、政府信息系统安全检查、电子政务外网安全建设等工作的逐步深入，各级政府机关单位对网络、信息安全的需求也日益增长，政府部门信息系统安全建设力度日益增强。

甘肃省作为国家西部省份，政务系统信息安全建设的担子尤其繁重，目前省内各级政府正处于政府外网建设、等级保护建设等重大项目规划阶段，为了促进和加强政府用户对系统安全建设的决心和信心，为各级政府领导规划 2011 年网络信息安全建设提供有力的预算依据，绿盟科技联手甘肃海丰举办了此次会议。

绿盟科技作为国内网络信息安全领域的领导者，长期从事等级保护实践工作，协助各行业用户开展等级保护咨询、建设、整改等工作，同时作为各地测评机构、检查机构的技术支撑队伍，积极参与了各行业、各地测评中心的体系建设，在这个过程中积累了丰富的实践经验。绿盟科技孙铁也是国家信息安全等级保护安全建设指导专家委员会专家。

会上，绿盟科技孙铁从当前国家各级主管机构应对目前严峻的网络安全态势所开展的工作作为出发点，针对不同的政府客户群体，从政府网络信息系统安全检查、政府网站安全建设、电子政务外网安全保障及等级保护工作等几个方面介绍了绿盟科技在其中所具备的技术实力以及成功应用的典型案例。从“点-平台-面”介绍了绿盟科技政府行业整体安全设计及保障思路，同时也和与会嘉宾交流了绿盟科技正在进行的政府信息安全方面的前沿研究课题。

华为发力行业信息化应用 产品方案覆盖七大行业

来源:电脑商情在线

目前,行业信息化已成为华为公司战略发展的重要方向,在近日收官的华为行业全国巡展上,华为中国区行业市场部部长陆隽表示,行业市场已成为未来华为一个新的增长点,公司将投入更多资源,助力行业信息化登高。

据了解,目前华为针对行业市场已投入更多资源进行市场服务,其中包括独立的后端研发组织,前端销售服务组织,同时华为还建立了面向全球的企业业务部,专注于服务全球企业以及行业客户。

与传统企业解决方案不同,华为在本次行业全国巡展中展示了包括基础网络、信息应用化应用、物联网等一站式融合解决方案产品,其中在中国区行业市场部作为落地国内服务行业的组织,主要服务政府、金融、广电、电力、能源、交通、企业等信息化建设。据了解,此次行业巡展活动历时 7 个月,覆盖全国北京、上海、广州等 27 个重点城市。

同时针对行业信息化部署方面,华为以北京为中心,联合国内 27 个代表处的网络服务平台资源,专职服务行业信息化的建设,而在深圳、北京、南京、成都、杭州、西安设立了 6 个专门的研发机构,面向行业信息化需求,提供不断满足客户需求的端到端解决方案。

在产品方案方面,华为此次发布了全新的企业网解决方案理念“网络新世界”,以及基于此架构的多行业解决方案,包括智能电网配网自动化、轨道交通一体化通信、广电三网融合、电子政务、数字城市、企业信息化。

在政府和企业行业,通讯、数据、应用融合的政企信息化解决方案首当其冲,其中主要包括数据承载、视讯、统一通信、呼叫中心、数据中心、安全一体化为主要解决方案内容。而在电力行业方面则以无线和有线技术为主,提供系列智能电网解决方案,涵盖输电、配电、用电环节。

“华为未来将以云计算为战略核心,推进数据中心、物联网、智能电网、公共安全应急等行业热点深入研究,重点推进行业标准,从而推进行业信息化的标准进程。”陆隽指出。

技术前沿

安全和普及是对立的么？

来源：zdnet 安全频道

在信息技术专家和软件铁杆拥护者之间接下来进行的讨论中，一个观点被不断提起，这就是：一种软件的受欢迎程度和安全性成反比。这一假设的逻辑是，随着软件的不普及，作为目标的价值就越大越具有诱惑力，而作为更具诱惑力的目标，会导致安全性进一步下降。

这种观点中存在一定的合理性，不过远远没有很多人想的那么多。如果在所有因素都相同的情况下，最流行的软件将首先遇到攻击，这是事实。但是，从另一方面来看，所有因素都相同的情况是不可能出现的，占据领先地位也不一定是必然：

在最流行的软件受到关注后，第二流行的软件也受到关注，如果它具有足够的安装基础的话，也可能成为攻击的目标。

对于软件市场来说，不需要多大的份额就足够进行攻击了。对于使用最广泛的软件来说，一个百分点就意味着数百万份的部署。

在其它因素相同的情况下，应用在高价值目标上的软件更容易受到关注。这种软件通常不是最流行的软件。

在其它因素相同的情况下，应用最广泛的软件可以被攻击者当作入侵其它系统的出发点而首先受到关注。如果没有其它原因的话，它说明了在使用更广泛的软件上进行的攻击范围更大。

实际上，第二流行的网络服务器软件远远没有最流行的网络服务器软件安全。

将所有这些事实综合起来的话，就会发现普及是导致安全下降的直接因素这一概念与推论之间出现了矛盾。上面五点中的最后一点，就是一个反例。声称的原因，不支持相关的推论，事实和论点之间产生冲突。毕竟，存在相关性并不等于存在因果关系。

当然，也可以从另外一种角度来看待普及性和安全性之间的关联。尽管普及性不是导致安全下降的直接原因，但是可以会给安全记录带来一定的影响。

在大多数情况下，这种影响不足以吸引坏人攻击更受欢迎的系统。如果绝大多数系统都部署成为非常安全的系统的话，对于很多恶意安全黑客来说，他们会更倾向于选择其它不那么受欢迎但更容易攻击的目标系统。

普及性对安全性带来影响是通过大量用户对系统设计带来的环岛效果而造成的。由于越来越多的人大声地要求得到某种功能或进行界面的调整，而为了安抚他们，开发商面临着越来越大的压力。这样下去就很容易导致在安全设计方面考虑的不是那么全面，导致复杂性飞速上升，开发方向出现错误。通常情况下，安全性低下的臃肿软件就这么出现了。

从全球范围来看，对于最终用户来说，微软 Windows 是最流行的通用操作系统。而取决于你询问的对象，及选择如何计算的假定，苹果的 MacOS X 是第二流行的。如果必须猜测一下的话，canonical 的 Ubuntu Linux 操作系统可以说是第三。有趣的是，这也是它们在安全问题方面的排名。

在处理潜在威胁方面，微软 Windows 的记录非常差。它使用的还是对安全没有足够重视的架构，基于“越大越好”而不是认识到简洁和安全之间关系的“越少越好”的原则。这样的原则加上在设计方面的问题，很容易导致小缺陷产生大灾难。尽管微软已经开始采取大量措施重点解决安全问题，但大量错误的安全策略，无数的膨胀功能以及设计方面的缺陷，加上现实环境让这一切几乎不可能成功。

苹果 Mac os X 是建立在一个更强大的核心架构下的，它包括了一个微内核，一个主要基于 bsd unix 用户态下的图形用户界面以及在 90 年代收购未来 (next) 软件时直接获得的专业级创新应用程序接口 (API)。尽管如此，苹果严格的策略（在某些情况下是基于“控制狂”模式，故意忽略其它人）破坏了良好的基础导致 MAC OS X 在安全方面不佳。表现就是在很多情况下，对安全漏洞的反应非常迟缓，也不合情理，比较起来微软 Windows 的补丁策略反而显得更好一些。

最后，让我们来看看 Canonica 的 Ubuntu Linux，随着一个个新版本的发行，它的体积也迅速膨胀开始接近我们所厌恶的微软旗舰操作系统。至少部分原因是它主要依赖于开放源代码模式的开发，并且这些项目往往具有较好的安全性，所以，Ubuntu 在安全方面面临的问题比 Mac os X 要小一些。不过，安全性下降依然是一个长期存在的问题。越来越大的软件，系统组件之间耦合的不断加强，以及为可以诱惑最终用户的表面性能而不是良好的系统设计提供更多的关注，所有这一切，导致系统日益接近它更受欢迎安全不佳的竞争对手。

相比之下，一些不太流行的操作系统在某种程度上依然关注设计正确性、自觉维护安全，并保持系统简洁合理和稳定，这可能也是它们不流行的原因。这些操作系统包括了：

Debian 和 Slackware 之类以技术为导向的 Linux 发行版本

“大众化”的 bsd unix 系统，Free BSD 最安全的 bsd unix 系统——关注正确性的 NET BSD 和关注安全审核的 OPEN BSD。

实际上，这也就是说，争论系统安不安全和普不普及是一样的。它们之间存在很大的相关性，并不等于普及程度和良好的系统设计之间存在冲突。不管怎么统计，即使最不流行的操作系统在全球也有上百万的用户，对于恶意安全黑客来说，也是非常有价值的目标了。实际上，由于具备更高的安全性，这些系统经常被用于面向工作的服务器上，在单个案例中，这让它们作为目标的价值更高。尽管这样，它们的安全记录却比微软 Windows、苹果 MacOS X 和 Ubuntu Linux 操作系统好的多。

只有在恶意安全黑客避免攻击第二和第三流行的选择，才能说明普及性和缺乏真正安全之间不存在关联。不过，它确实有关联，安全系统设计和维持会被普及性带来的社会压力所影响，导致实际安全被忽视。

重复数据删除技术 成备份容灾的利器

来源:万方数据

随着企业信息系统的不断发展,业务系统的不断增加,在提高了日常业务运营效率的同时,也极大增加了企业内部的数据负担。随着各系统数据量的快速增长、以及数据类型的不断丰富,企业的信息中心面临着系统数据完整性、安全性、可用性等方面的严峻挑战。必须能够确保各个系统的数据得到有效的保护,并在故障出现时迅速准确地予以恢复,以最大限度减小一切可能的损失,实现业务的正常运转。

数据的安全性保障包括多个方面,如防病毒、系统入侵检测、硬件故障、系统冗余、系统数据备份等,而数据备份是上述安全性保障最核心也是最重要的保障手段,因为它直接对用户的各种数据进行备份,从而达到数据保护的作用,当各种影响数据安全的情况发生时,能以最短的时间恢复受损的数据。采用先进的数据存储技术结合目前主流的数据备份、容灾技术及架构体系将成为企业数据保护的应用趋势。

一、重复数据删除技术原理

目前集团公司的备份系统虽然可以完成现有状况下的备份要求,但还是存在以下方面的不足。备份系统恢复难度大,备份机制不完善;备份数据的可恢复性和完整性没有办法 100%验证,已经备份的数据要负担极大的不可恢复的风险,而这个风险却又是无法预知的;日常备份业务的维护和管理涉及到备份软件、磁带库运行报告的监控,磁带的保存和管理,整体维护和管理成本偏高;在当前情况下,完成异地的备份数据复制需占用远程链路,如采用本地盘阵,成本将非常昂贵。

备份数据中一般会包含很多的冗余,而当我们某一周的全备份镜像和其随后的各个周的全备份镜像相比尤其如此。尽管增量备份只是取那些变化的文件,但增量备份中通常也会包含冗余的数据块。容量优化(Capacity Optimization)是通过分析数据中的独特重复模式,然后把它用更短的符号表示,从而在存储介质中可以存储更多数据的一种技术。当数据写入到备份存储设备时,数据会被分成可变长度的数据段,也可以说一序列的字节。容量优化技术会实时将该数据段与已经存储的各数据段做比较。这种方式保证每个唯一独特的数据段只保留一份。所以容量优化技术可以在文件内或文件间,甚至是数据块内,发现重复的文件和数据段。实际所需的存储空间也就相对于所保存的数据量低一个数据量级。

容量优化有效率的关键是不依赖于数据格式,全局压缩技术可以应用到任意类型的重复数据——结构化数据(比如数据库)或者非结构化数据(比如文本文件,存储在文件系统上的数据)。不管什么样的数据格式,都可以实现高效率的备份。全局压缩算法会对所有要存放在备份设备上的数据做分析,而不管数据的格式和排列方式如何。优化的好处随着时间的推移会越来越明显。对于压缩效果最大的一个影响是备份策略。全备份相对于增量备份的重复度更高;越多的全备份越能够加剧压缩效率。假设是每周全备结合每天的增量备份的话,经过四个星期,预计压缩率可以达到 10:1。八个星期

后, 预计压缩率为 14 倍。在 18 个星期后可以达到 20 的压缩率。影响压缩效果的另一个因素是数据本身。例如, 一份工程设计过程文档的备份镜像, 包含多份副本文件或相似文件(一个文件被拷贝很多次, 各个版本间的变化很小), 显然容量优化利于应用于这种数据。

二、备份容灾系统能够实现的目标

2.1 能够实现集中容灾模式

通过支持容灾资源的集中模式, 实现一对多的数据集中容灾。对各客户端容灾数据以透明的方式自动同步到集中容灾中心。在用户需要恢复数据时, 可以通过简单的操作, 将数据自动恢复到本地。

2.2 能够灵活制定传输策略

根据用户业务要求, 统一制定灵活的传输策略, 支持按天、按时、实时等多种传输策略。

2.3 能够对集中容灾平台进行全面管理

在集中容灾中心实现数据的集中存储、集中管理、安全监控、作业监控。提供各用户信息中心容灾设施的部署、配置、运维、恢复等全程管理功能。具有较强的日志功能, 随时记录备份用户信息、备份执行隋况、恢复隋况以及系统运行状况等。

2.4 能够实现远程容灾功能

数据备份采用无人值守操作, 无须人工执行和干预。通过容灾数据的自动远程传输, 包括支持增量传输和断点续传, 实现抵御大范围灾难事件的能力。

2.5 能够实现数据的优化存储和优化传输功能

能够以较小的物理存储容量存储更多数据, 节省存储容量。同时, 在优化存储的基础上, 只传输变化的数据, 节省容灾数据传输带宽的成本。

2.6 能够实现数据安全保证功能

支持用户自己选择加密, 确保数据仅用户可访问。通过持续数据校验, 确保数据存储可靠。支持数据校验, 确保数据的一致性和可恢复性。

结合前面所论述的现状与技术路线, 可以设计出备份容灾解决方案。整体方案采用基于磁盘介质、具备高压缩能力(20: 1)的虚拟磁带库产品作为核心备份设备, 总部负责完成数据备份, 并接受其他分公司和项目部复制到总部的数据。分公司或项目部完成本地的数据备份, 并将数据复制到总部。总部使用现有备份软件, 结合虚拟磁带库, 构建成面向快速恢复的数据备份容灾系统。所有应用服务器可以将数据按照既定策略高速备份到虚拟磁带库上。在未来数据中心建成后, 新中心可和容灾系统构建成面向快速恢复的 3 级数据备份容灾系统体系。

由于采用容量优化技术, 与其他基于磁盘的备份系统相比, 其通过广域网传输的数据量减少了 95% 以上, 使得将数据备份到磁盘成了可能。由于可以存储整个数据备份保留周期内的所有备份数据, 从而使磁盘备份的优越读写性能得以贯穿整个备份周期, 如果必要的话, 数据可以通过网络以同样的效率从异地的复制端恢复, 或者将异地的数据直接在异地恢复。复制性能远远高于实际物理

链接所能够提供的性能，从而进一步降低总体成本。

三、结束语

基于重复数据删除技术的数据备份和容灾方案，既具备磁带的经济性，又具备磁盘的可用性和速度，同时克服了磁带和传统磁盘存储阵列固有的缺陷。该解决方案的成本不高于磁带自动化的方案。同时满足不断增长的数据量要求，实现高性能的备份和恢复。解决方案比传统 RAID 和文件系统具有更高级别的硬件和软件保护能力，提供了可验证的可恢复性和高弹性的存储。

黑客攻防

年末黑客扎堆盯网购 木马作者月赚百万

来源:赛迪网

年终岁末，伴随着网购市场的异常火爆，大量病毒木马鱼贯而出，纷纷扎堆年末的网购市场，伺机展开赤裸裸的“抢钱”行为。据安全专家李铁军预测，未来一个月内，新增与网购相关的钓鱼网站将超过 5 万个，预计波及网民累计将达千万人次。

李铁军指出，年终岁末，圣诞元旦购物季期间，黑客针对网购的安全攻击主要包含三大类：钓鱼网站、新型交易劫持木马、传统盗号木马。其中，钓鱼网站、新型交易劫持木马将成为本次网购高峰的主要威胁。

据《2010 年中国网络购物安全报告》显示，2010 年网络购物安全形势非常严峻，日新增网购相关的钓鱼网站多达 1500 多个，而新型交易劫持木马的增长更为迅速，从最初的 1 个快速发展至千个，日攻击网友数量也已超过 2000 人次。

报告显示，新型交易劫持木马是一种技术含量非常高的木马，一对一的传播方式，导致了该木马作案成功率非常高。而很多网民因为损失数额不多，在举证以及后期的案件追踪等方面都存在一定难度，因此也助长了此类木马的嚣张气焰。

以数字大盗木马为例，作为新型交易劫持木马的典型代表，数字大盗木马虽然目前仍然没有大面积扩散，而点对点的传播也使木马作者隐藏的更深。金山网络安全中心担心该木马的攻击方式如果公开，将会对在线购物安全构成严重威胁。

据了解，以数字大盗为代表的新型交易劫持木马的作案流程基本一致：在交易过程中，买家执行了对方发过来的文件（木马），在继续交易时，木马会创建一个新的隐藏的交易单，这个交易单会抢在正常交易单之前被提交。在整个过程中，买家完全看不到交易信息被篡改，会直接将货款打到

犯罪分子指定的帐号中。据李铁军保守估计,仅数字大盗一个木马,从今年 6 月份被发现至今,至少敛财上千万元。

圣诞节、元旦、春节接踵而至,网购市场的火爆也给病毒木马作者提供了更多敛财的机会。为了保障广大网民的网络购物安全,安全专家建议广大网民:1、安装专业的安全防护软件,开启实时监控功能,实时防护网络攻击;2、安装安全辅助类工具,及时修复电脑内的安全漏洞,不给病毒木马以可乘之机;3、网络购物过程中,仔细辨别网址、不随便接受陌生人传送的文件,以防遭遇钓鱼、木马攻击。

打击黑客: 需要以彼之道 还彼之身

来源:新智囊

正如黑客形成地下产业链一样,全社会的企业、厂商和政府也要协同工作,形成针锋相对的产业链,才能击败黑客犯罪集团这一共同的敌人

时下,腾讯 QQ 与奇虎 360 之间的“恶斗”把“网络安全”炒得火热。

事实上,网络安全领域从来都不太平。从瑞星与金山的口水战,到 360 与瑞星、金山之间的官司,现在战火燃至腾讯,起因也在网络安全领域。

应该说,安全问题是现在最为火热的话题之一,日前,在 RSA 大会 2010 信息安全国际论坛上,云计算安全、可信计算、反网络欺诈、法规遵从和密码学五大议题成为中国信息安全界最关心的、最热门的话题。

EMC 全球执行副总裁、RSA 全球总裁亚瑟·W·科维洛(Arthur W. Coviello, Jr.)认为,人们对于信息安全问题的担心,已经非常严重地影响了企业部署云计算的步伐。

像“黑客”一样思考

科维洛表示,新一轮经济增长的动力是云计算,但是由于安全的问题没有解决,目前人们对云计算缺乏信心。科维洛先生指出,解决云计算的安全问题,需要采取综合的、系统化的、内嵌的安全方式。正如黑客形成地下产业链一样,全社会的企业、厂商和政府也要协同工作,形成针锋相对的产业链,才能击败黑客犯罪集团这一共同的敌人。

科维洛认为,网络安全面临着三大方面的挑战——

首先,我们面对的问题就是安全措施被动的应用,我们查补漏洞,我们看到新的形式的攻击,我们有新的单点产品解决问题。这说明我们有很多的单点产品来自不同的供应商,都是独立运用的,比如加密、解密、反恶意软件、网关等等,由此 IT 团队也需要担负管理多家供应商提供的产品的责任。这样耗资巨大,而且是抵消的,是无法管理的,这就是面对的第一个问题。

其次,比起软硬件单纯的物理环境,虚拟化让安全管理和控制变得更加艰难。

再有,我们面临着非常复杂的、越来越程度越高的犯罪和黑客社区。

网络威胁已经超越国界,成为一个不争的事实。根据 RSA 反网络欺诈指挥中心的研究,2010 年中国网络钓鱼的数量上升了 78%。99%的网络钓鱼指向网上购物。中国国家互联网应急中心(CNCERT)发布的报告也显示,2010 年上半年 CNCERT 共接到网页仿冒事件报告 740 次,经归类合并后具体成功处理了 308 件,被仿冒的网站大多是国外的著名金融交易机构。2010 年上半年中国大陆地区有 23.3 万个 IP 地址对应主机被僵尸程序控制;参与控制中国大陆计算机的境外僵尸网络控制服务器 IP 有 4584 个,主要来自美国、土耳其和印度。

云计算在给人们带来便利的同时,也会给黑客带来“便利”。黑客可以利用云计算资源,研究出更有创新性、更高效的攻击方法。比如个性化的定制攻击,会伪装成人们的朋友、亲人,通过 Twitter、Facebook、开心网等发起让人很难察觉的网络攻击。

黑客正在不断改变攻击方式,这就需要人们同样要有“黑客式”的思维方式,从黑客的角度去看安全,这样才能发现潜藏的威胁。现在的软件愈发复杂化,黑客的攻击手段也愈发多样化,这就需要打破以往固有的范式,要像黑客一样思维。

信息安全是管理问题

而非单纯的技术问题

近年来,企业的经营愈来愈困难。除了经济景气的循环之外,天灾人祸频仍,让企业的营运更加困难。在这样的环境下,如何让营运不中断,成为企业最重要的课题之一。当灾害来临时,能持续营运而不中断的企业,才能保有其竞争力。除了地震、洪水、非典以及禽流感等天灾之外,企业营运大量仰赖信息以及网络系统,也让信息安全上的灾害,成为中断企业营运,造成严重损失的重大人祸之一。

这些信息安全管理上的难题,往往并非企业中的信息部门人员可以独力解决的。许多企业将所有的问题归咎于信息部门人员,不但不公平,同时也无法真正解决问题。信息部门多样而繁杂的工作,以及有限的人力,使得信息安全管理的工作,成为其沉重而无法独力承担的责任。

RSA 公司 CISSP、CISM、eGRC 解决方案经理 Steve Schlarman 认为,对很多大企业来说,无论在基础架构、网络、数据库等方面,都能找到造成漏洞的根本的原因——人,人的治理对企业的数据安全是至关重要的。因为对于操作键盘的个案来说,你一定要让员工清楚你对他们的要求是什么,他们要得到指导,之后才能确保企业的安全。有这样一个例子,一个员工不太了解业务流程保护,不小心把企业信息泄露给外界团队,这个团体被指控为欺诈罪。我们在实践中发现有时候并不是技术导致问题,而是管理的漏洞。所以我们强调技术加人,一是提高人们的保护意识,二是使我们有一个开放环境进一步沟通。比如我们在有关的业务流程中,大家应该知道有什么样的控制因素、控制措施,这样能防患于未然。

Steve Schlarman 回顾说,信息安全行业在过去 15 年中发生了很大的变化,原来只有几个人针对技术问题进行研究,后来涉及面越来越广,我们需要对信息安全、隐私等方面从整个企业层面上构置架构,面对全面的挑战。

应该说,在今日的企业环境中,信息安全的问题,已由技术层面,扩大到管理层面。唯有正视信息安

全的管理问题,寻求信息安全专家的专业服务及帮助,才能真正解决企业的信息安全问题,同时维持企业营运的不中断。

黑客热衷入侵政府类网站：技术成本低 收益高

来源:北京日报

济南市公安局成功侦破一起新型制售假证大案。犯罪分子采取黑客攻击手段,入侵国家级教育网站和多所高校网站,篡改数据后大肆制作和销售假学历、假证书。

新闻背景

今年 12 月中旬,两名仅有初中学历的 90 后,因非法侵入最高人民检察院反渎职侵权厅网站后台、非法控制长沙质量技术监督局等政府网站,涉嫌构成非法侵入计算机信息系统罪、非法控制计算机信息系统罪被公诉至北京市朝阳区法院。

然而,这绝不是个案。据国家互联网应急中心的监测报告显示,2010 年 5 月 10 日至 16 日,仅一周内,中国境内就有 81 个政府网站被篡改,其中包括 4 个省部级网站,还有 25 个地市级政府网站。为何政府网站频频被黑?根源究竟在哪里?黑客和其掮客将被追究哪些刑事责任?

黑客为何“偏爱”政府网站

当今的网络发展可谓百舸争流、百花齐放,网站不仅是绝对数量大,而且种类繁多、形式多样,既有营利性的商业网站,也有服务性的企事业单位、政府机关网站。然而,在众多网站中为何政府网站屡屡被黑呢?

据了解内情的专业人士介绍,黑客“偏爱”政府网站主要有两方面原因:一是政府类网页搜索引擎给的评权重、网页级别高,黑这类网站易于获得更高的搜索排名、更高的点击率,可以赚更多的钱;二是政府网站尤其是基层政府网站技术力量薄弱,从成本与收益角度来讲,简单说就是“成本”低、“收益”高。

除了上述两种原因,还有一种原因也不可忽视,那就是部分政府网站发布商家的负面消息,如某企业的不良信用评价等,为了删除这种不利消息,部分商家不惜花高价请黑客攻击政府网站,这也是此类政府网站屡屡被黑的重要原因。

“黑客产业链”悄然兴起

政府网站频频被黑,网络安全受到巨大威胁,幕后的真正推手,是悄然兴起的“黑客产业链”。

黑客是指利用计算机信息系统安全漏洞非法侵入、控制、破坏计算机信息系统的人。黑客源自英文单词 hacker,原意指用斧头砍柴的工人,最初的黑客是指专门研究、发现计算机和网络安全漏洞的计算机爱好者。

随着计算机网络信息技术的高速发展,计算机网络产值也在逐年攀升,在网络利益逐渐多元化

的过程中，发展中的黑客群体也呈现多元化趋势，如今有恶作剧黑客，也有政治性黑客，而值得关注的是营利性黑客的出现。他们专门利用计算机网络信息安全漏洞谋利，目前营利性黑客队伍正在逐步形成并壮大。

更为可怕的是营利性黑客盈利方式的“产业化”，当黑客们编写的木马病毒程序或黑客行为成为“商品”并进行流通时，由此衍生的“黑客产业链”悄然形成。

在这条产业链形成的产销关系中，“生产者”负责编写木马病毒程序，“销售商”订制或购进病毒商品而后进行倒卖，“消费者”向销售商购买或预订病毒程序，而后利用病毒工具实施网络攻击。他们主要采用种植“暗链接”以提高目标网站点击率，非法获取他人信息，删除政府网上对商家不利的信息等。

另外，黑客行为也可能成为“商品”，中间商负责在黑客与需要黑网站的客户之间牵线搭桥，促成客户雇用黑客黑网站交易的完成。

通过上述产业链的运作，多方实现了非法盈利，而对网络安全的破坏作用呈几何倍数增长，“黑客产业链”的形成严重危及网络安全，已经成为正在恶化、急需惩治的社会问题。

危害网络安全谁担刑责

面对严峻的网络安全形势，2009 年通过并实施的刑法修正案七新增了两款规范打击计算机网络犯罪的规定，新增了非法获取计算机信息系统信息罪、非法控制计算机信息系统罪以及提供用于侵入、非法控制计算机信息系统的程序、工具罪三个罪名，加上原有的非法侵入计算机信息系统罪、非法破坏计算机信息系统罪，一共有五个罪名入刑。

从处罚力度来看，刑法修正案七加大了打击计算机网络犯罪的力度，一般判处 3 年或是 5 年以下有期徒刑、拘役，单罪最高可判处 15 年有期徒刑，尤其是新增罪名均可并处或单处罚金，可见立法上加大了对营利性黑客利用网络安全漏洞谋利行为的打击力度。

在“黑客产业链”中谁有可能被追究刑事责任呢？

一是攻击计算机信息系统的黑客 主要包括以下行为的实施者：违反国家规定侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的行为；违反国家规定破坏计算机信息系统的行为；非法获取计算机信息系统数据的行为；非法控制计算机信息系统的行为。

二是黑客行为的协助者 他们虽然不直接实施黑客行为，却是黑客行为的协助者，主要包含两类：一类是木马病毒程序、工具的提供者。提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具的行为人，情节严重的，都将以刑法修正案七新设的提供用于侵入、非法控制计算机信息系统的程序、工具罪追究刑事责任。

第二类是虽不提供程序或工具但协助黑客行为的实施者。明知他人实施计算机类犯罪行为仍为其提供帮助的，应按黑客所犯罪的共犯处罚。这样，“黑客产业链”中即使不直接实施黑客攻击行为的“生产者”、“销售者”、负责联络的中间商以及黑客雇佣者，都是有可能被追究刑事责任的。

美国银行决定买下员工域名 防止域名被黑客利用

来源:CCID

据外国媒体报道,美国银行(The Bank of America)目前已经决定全部买下员工的域名,以防止域名落入黑客之手。而此举也被外界解读为美国银行担心黑客将会根据员工的名字买入其域名,从而在域名上发送色情信息和恶意软件。

此前,维基解密网站创办人朱利安·阿桑奇(Julian Assange)在接受《泰晤士报》采访时曾表示,他手头上持有足够多的美国主要银行的负面资料,将能够迫使银行的高层管理人辞职。虽然阿桑奇并未言明是哪一家银行,但是维基解密极有可能通过其相应设备获取到美国银行的内部文件和邮件。由于市场猜测美国银行将成为维基解密下一个高调攻击的目标,美国银行在阿桑奇发表言论的当天股价一度下跌 3.18%。业内人士分析指出,美国银行此举表明自身已制定出相应策略,对维基解密将有可能发布的内部文件予以有力回击。

根据域名信息网站(Domain Name Wire),美国银行首席执行长莫伊尼汉(Brian Moynihan)的域名目前已遭受攻击。为此,维基解密向该行的顾客建议,应该把钱存放在其它更安全的地方。此前,美国银行曾与 Visa, MasterCard 和 PayPal 共同拒绝了为维基解密提供金融服务。

360 密盘不足 2 月被黑客攻破 金山推补丁忙修补

来源: DoNews

Donews12 月 30 日消息 12 月 30 日晚间,曾宣称 10 万年才能被攻破的 360 密盘产品不足两月便被黑客拿下,一位匿名黑客针对 360 密盘开发了一款专门的解锁软件,可以在瞬间解密任何被 360 密盘保护的文档。此间,另一家国内安全公司金山网络今日晚间就此紧急推出相关补丁。

据该匿名黑客表示,此次攻陷 360 密盘不是利用了程序 Bug,而是利用了 360 密盘本身设计上的缺陷。“360 密盘只是一个用 FileDisk 源代码修改出来的东西。”他表示。该黑客还调侃的表示,“估计这个东西的开发 team 这两天不会好过,希望你们别怪我,怪你们喜欢吹牛的老大和给力的宣传吧。”

国内另一家安全公司金山网络则在今日晚间紧急推出相关补丁,据金山网络相关人士表示,鉴于该黑客的破解工具可能被别有用心的恶意利用,而迄今有很多用户也并不知道 360 密盘已被攻破这一情况,金山网络决定提供补丁程序,帮助 360 密盘用户的防止隐私泄露。

金山网络拒绝对此次事件进一步置评,仅表示推出补丁程序旨在保护网民机密信息不被黑客侵犯,全方位保护网民个人隐私,不愿意卷入任何可能发生的口水战。

微软警告黑客利用 Word 缺陷在 PC 中植入恶意插件

来源:腾讯科技

北京时间 12 月 31 日消息, 据国外媒体报道, 微软当地时间周二表示, 黑客在利用 Word 中一处缺陷在 Windows PC 中植入恶意件。

微软 11 月 9 日发布的补丁软件修正了 Word 2002、2003、2007 和 2010 中的该缺陷, Mac 版 Word 2004 中的该缺陷没有得到修正。但是, 目前的攻击仅影响 Windows 版本。

微软恶意件保护中心研究人员罗德·费诺尼斯(Rodel Finones)表示, 黑客利用恶意 RTF 文件, 造成 Windows 版 Word 出现栈溢出。攻击得手后, 恶意代码会下载到 PC 上, 并运行一个特洛伊木马病毒。

上个月, 微软将 Word 2007 和 2010 中 RTF 缺陷的危险等级评为“危急”, 将其他版本中的 RTF 缺陷危险等级评为“重要”。

当时, 外部研究人员称, 黑客可能选择利用 RTF 缺陷兴风作浪, 因为用户只要在 Outlook 电子邮件客户端中预览恶意 RTF 文档就会中招。

费诺尼斯呼吁用户尽快安装微软 11 月份发布的补丁软件。

海外来风

More Mac malware common on 2011 prediction lists

来源: scmagazineus 杂志

Will 2011 be the year that threats against Mac platforms and devices finally reach the tipping point?

Yes, according to a number of security firms.

McAfee, in its annual list prognosticating what next year holds from an information security perspective, believes that Apple-targeted malware will increase in sophistication.

"Historically, the Mac OS platform has remained relatively unscathed by malicious attackers, but...the popularity of iPads and iPhones in business environments, combined with the lack of user understanding of proper security for these devices, will increase the risk for data and identity exposure, and will make Apple botnets and trojans a common occurrence," the company said Tuesday.

Meanwhile, PandaLabs predicts a similar increase in threats, especially as the market share for Mac users grows.

"The greatest concern is the number of security holes in the Apple operating system," the company said. "Developers will need to patch these holes as soon as possible, as hackers are well aware of the possibilities that these vulnerabilities offer for propagating malware."

CoreTrace, an application whitelisting firm, foresees considerably more exploits in 2011 aimed at mobile devices, such as those running Apple iOS, the specialized version of Mac OS X.

Threats geared for the Mac are not unheard of, but Apple users have been more likely to be hit by a phishing attack than malware in the past.

Apple's media relations department is closed for the holidays, and a representative did not immediately respond to a request for comment.

2011 年预测 Mac 上将会出现更多的恶意软件

来源：scmagazineus 杂志

——中国信息安全博士网翻译

2011 年将是针对 Mac 平台和设备的攻击年，最后能到达以往的最高点吗？

根据企业的数据反映，这答案是肯定的。

迈克菲在其年度总结中列出了明年的安全预测，相信明年苹果将会增加针对恶意软件的复杂性的防范。

“从历史上看，在 Mac OS 平台遭到恶意攻击时，相对来说还是毫发无损，但是 ipad 公司 iPhone 手机在其商业中的普及，随着用户对这些设备应用但是又缺少安全的意识，将会增加对数据和身份曝光的风险，这将导致苹果僵尸网络和木马经常发生”，该公司在星期二说。

与此同时，熊猫病毒实验室预测随着 Mac 用户市场份额的增加，类似的威胁将会增加。

该公司表示：“现在最大的担忧就是苹果操作系统的安全漏洞数量还是未知，开发人员需要尽快的修补这些漏洞，因为黑客有可能利用这些漏洞传播恶意软件”。

CoreTrace 公司是个应用程序公司，该公司预测 2011 苹果的漏洞相当多，例如针对那些移动设备苹果内部监督办公室的 Mac OS X 的版本。

Mac 遭到攻击并不是没有，比如苹果用户已经或者更可能被一个过去的恶意软件所命中。

苹果公司的媒体部门并没有代表对此事做出回应。

企业推荐

国工信科技发展（北京）有限公司

国工信科技发展（北京）有限公司是一家致力于信息集成服务和提供信息安全培训产品的高科技企业。公司旨在为政府、军队、军工、专业院校等高端客户提供信息情报的集成服务、信息网络安全的专业咨询以及虚拟信息社会的现实展现服务。

公司拥有一批高素质的理论专家和技术开发团队，主要成员是来自中科院、北京大学、北京交通大学、国防科技大学、社科院等著名高校和科研院所的专家、博士。

伴随第四次信息技术革命的迅猛发展，信息化在全球得以快速应用，以互联网为依托的虚拟社会渐进形成。公司专注于研究现实物质世界和虚拟网络化世界的融合发展，并在信息安全攻防展现及虚拟信息对抗展现方面取得了领先的研究成果，通过精准的客户服务，与国家关键核心部门和精英团体建立了高效的合作关系。

国工信公司将以精英客户需求为导向，以前瞻视角和理论为依托，重视技术与应用的完美结合，提高公司的核心企业竞争力，为客户提供一流的产品服务和解决方案，为共同塑造和谐世界而努力。

中国信息安全博士网

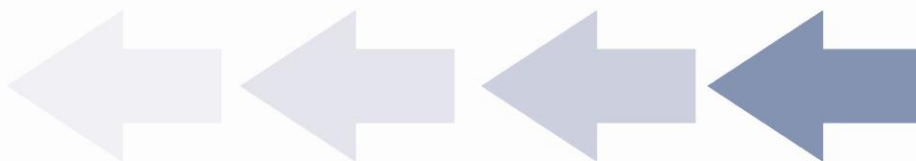
www.secdoctor.com



高端访谈

聆听信息安全 访谈高端人物

中国信息安全博士网作为中国信息安全行业的高端智库平台，一直在我国信息安全行业发展过程中贡献着自己的力量。智慧的对话，思想的交锋。政府官员、专家学者、社会名人、国际友人做客中国访谈，解读政策法规，阐释新闻热点，讲述世界风云，倾诉人生故事。秉承权威、人文、开放、深入的原则，为网友展现不同人生的精彩历程。为行业发展、产业进步提供建议。将客户的相关文字、音频或视频文件放在中国信息安全博士网高端访谈栏目进行宣传。



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: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
E-mail: Security@inspur.com