

安全周报

中国信息安全博士网

九月 第三期

二〇一〇年九月二十六日
总第26期

weekly.secdotor.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



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。

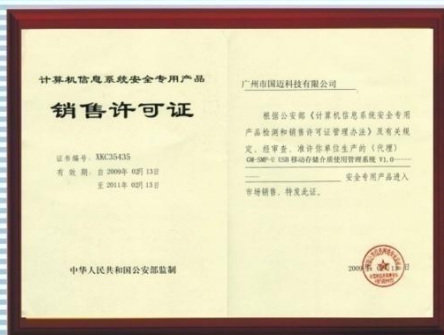
■ 专用安全U盘：

内部U盘、单向导入U盘、单向导出U盘、双向交换U盘。

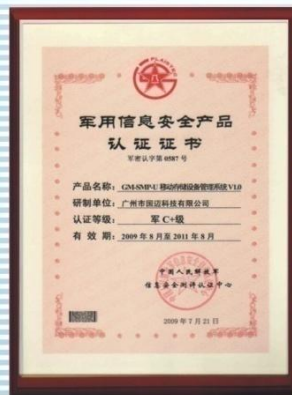
权威认证：



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.guogongxin.com> email: secdoctor007@163.com



第二届中国信息技术及信息安全 人才培养与就业工作研讨暨交流会

(北京 · 2010年12月18日-19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

主办单位： 教育部高等学校信息安全类专业教学指导委员会

联合承办： 中央财经大学
北京理工大学
中国传媒大学

协办单位： 北京电子科技学院
北京信息科技大学
北京交通大学

支持媒体： 大学生就业网、中华英才网、智联招聘、赛迪网、中国计算机安全网、
天极网、计世网、 信息网络安全、计算机安全杂志、信息技术与信息安全

会议主题： 新形势下信息技术及信息安全人才需求与就业

届时，教育部、工业和信息化部领导，国防、军工、IT厂商、信息安全厂商等用人单位及全国各大名校师生齐聚北京。

欢迎各界用人单位踊跃报名：

会 务 组 ： 010-64126291 13661116129 张鹏飞

电子邮箱 ： cis-rc@163.com

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.secdactor.com

目录

学术会议.....	7
黑客安全会议：互联网造就摇滚以来最大代沟.....	7
第一届中国认证认可信息网专家论坛在京举办.....	7
广州市人大常委会机关召开保密工作会议.....	8
政府之声.....	9
网络安全问题涉及多方 需要政府介入支持.....	9
全球网络协议草案出炉.....	11
美信息安全战略跨入 3.0 时代.....	12
捷克为保护公众隐私拒绝谷歌 Street View 申请.....	13
国家标准化委员会批准 18 项信息安全标准.....	14
病毒播报.....	16
Linux 内核中的漏洞提供了非法根权限.....	16
报告称 Facebook 是最危险社交网站.....	16
中秋期间上网需防范间谍木马病毒窃密.....	17
Adobe 发布补丁修复 Flash 播放器漏洞.....	18
超级病毒疑似攻击伊朗核电站 疑是国家行为.....	18
订机票慎防航空公司“山寨网”.....	19
瑞星称 Stuxnet 病毒全球肆虐.....	20
QQ 为推产品谎报漏洞.....	21
安全漏洞发现情况周报表.....	22
产业动态.....	58
国家测绘局：2015 年可全国虚拟旅游.....	58
谷歌街景服务在德国遇到强烈抵制 上万人退出.....	60
惠普完成对 Fortify Software 并购.....	61
Facebook 称数据库软件问题导致严重故障.....	61
新版阿里旺旺可识别木马 将于一个月内面世.....	62
谷歌微软和 IBM 竞标美国联邦总务局云计算合同.....	64
安全市场面临重新洗牌.....	64
华为将史无前例地向客户开放其计算机源代码.....	66
微软敦促电子隐私法案 以助云计算等新技术的发展.....	67
技术前沿.....	68
《科学》：多国科学家首次实现双光子的量子游走.....	68
数据中心制冷技术面临的新挑战.....	68

黑客攻防	70
Dos 采用 web 服务器攻击	70
“日本国防部被黑客攻击”疑似骗钱	71
警惕黑客破坏网络安全	72
篡改 Comcast 网站黑客获刑 18 个月	73
委内瑞拉总统查韦斯 Twitter 账户疑遭黑客入侵	73
黑客发动恶意攻击更具隐蔽性	74
海外来风	75
One million malware-infected spam HMTLs appearing every day says Barracuda Networks	75
高端访谈	77
高端访谈下期预告：专访王昭顺教授	77
企业推荐	78
广州市国迈科技有限公司	78

学术会议

黑客安全会议：互联网造就摇滚以来最大代沟

来源：新浪科技

北京时间 9 月 20 日上午消息，据国外媒体报道，黑客安全问题会议“Hacktivity2010”于周日在匈牙利闭幕，本次会议讨论了如何应对日益复杂的互联网侵权行为。

在为期两天的会议上，来自美国的世界知名网络安全专家布鲁斯·施尼尔(Bruce Schneier)表示：“互联网造成了自摇滚以来的最大代沟。”

他说：“我们需要为生活在互联网上的新一代人做好准备，他们不知道电脑或智能手机与互联网的界线，与朋友分享密码以表现信任，并且在注册服务时故意说谎。”

他表示，由于目前的技术和商业趋势是减少对用户的控制，未来的互联网安全和隐私问题令人担忧。

本次会议共安排了大约 30 场演讲，与会者还探讨了数据库保护的问题，涉及 Oracle、MySQL、MSSQL、DB2 LUW、Sybase、ASE 和 PostgreSQL 等相关软件。

会议还讨论了 Web 2.0 的相关问题，Web 2.0 涉及人们对万维网使用方式的改变。前 Hacktivity 会议组织者、现任匈牙利兹里尼·米克洛什国防大学(Miklos Zrinyi National Defence University)研究人员 Csaba Krasznai 表示：“人们正越来越多地使用 Web 2.0 技术。”

他表示，Web 2.0 的威胁不仅影响到个人，而且危及企业 and 国家，并认为有必要“基于社会内部的变化”建立安全措施。

会议还讨论了 iPhone 和黑莓等手机的仿冒问题，匈牙利安全专家 Domonkos Tomcsanyi 表示，利用 PDA 或掌上电脑很容易仿冒这些产品。

第一届中国认证认可信息网专家论坛在京举办

文章来源：中国计算机安全

《中国国门时报》9 月 20 日，第一届中国认证认可信息网（以下简称“中认网”）专家论坛在京举办。与会专家希望中认网充分发挥作用，不断增大信息量和提高信息质量，更好地服务社会大众。国家认监委有关负责人向中认网专家委员会专家颁发了聘任证书。

国家认监委有关负责人对中认网的工作给予了充分肯定，并要求中认网通过认证认可工作的宣传，提高公众对认证认可工作的认知，提升对社会的影响力。据介绍，中认网是经国家认监委批准、

由国家认监委信息中心主办的认证认可行业门户网站,几年来为宣传认证认可政策、服务社会公众、坚持正确的舆论导向发挥了积极的作用。中认网从2003年正式上线运营开始,网站日均流量从3000次逐步增长到6万多次;网站日均独立IP从200个逐步增长到近4000个;网站用户从不足200名增长到6000多名。2009年秋季,中认网组建了“网站专家团队”,吸引了来自全国各地认证认可各业务领域的专家,这些专家汇集一起,为中国认证认可信息网的建设拓展思路,为认证认可事业的发展贡献力量。

与会专家还围绕着中认网如何更好地与认证认可事业融合、发展和创新,结合强制性产品认证、实验室认可与信息化管理、信息安全与认证认可的发展和食品农产品安全等多个领域进行了交流研讨。

广州市人大常委会机关召开保密工作会议

来源: 广州人大网

市人大常委会机关保密工作会议在801会议室召开。会议由副秘书长、机关保密委员会副主任汤抗美同志主持,各委办室分管保密工作的办公室领导及专兼职保密员参加了会议。

会上,汤抗美副秘书长传达了省委保密委会议精神;秘书处处长邓穗平同志传达了全市深入学习贯彻新《保密法》动员大会暨学习新《保密法》辅导报告会精神;秘书处鲍丽珊同志通报了我会机关开展新《保密法》学习宣传活动的情况;各部门保密工作人员互相交流,并就近期保密工作中存在的问题提出建议;汤抗美副秘书长就进一步做好下阶段的保密工作提出了要求。

汤抗美副秘书长指出,自1989年我国《保密法》颁布并施行,到2010年新修订的《保密法》的颁布,已逾20年,我国保密工作所面临的形势发生了深刻的变化,大家要增强保密的责任感和使命感,做好新形势下的保密工作。

一、认真学习贯彻落实新《保密法》

一是抓好新《保密法》的学习宣传工作,通过学习宣传,让新《保密法》深入人心,使广大干部群众特别是领导干部和涉密人员懂保密、会保密、善保密;二是对照新《保密法》查找工作的差距,并结合我会机关的工作实际,建立健全与之配套的保密规章制度;三是根据新《保密法》认真做好我会机关的保密工作,把法的精神、法的要求贯彻到实践中,落实到工作里。

二、重点抓好信息化条件下的保密工作

在信息化条件下,现代通信技术的迅猛发展和办公自动化设备的广泛应用,使泄密渠道不断增加,信息领域的窃密与反窃密的斗争更加复杂。近年一系列损失惨重的失泄密案件告诉我们,越来越多的失泄密案件与网络直接相关,网络已日益成为窃密和反窃密的主战场。在今后的保密检查中,要确保不漏一人、一机、一盘、一网,切实堵塞泄密漏洞。

三、正确处理好政务信息公开和做好保密工作之间的关系

近年来，政务公开的大力推行对于保密工作提出了更高的要求。我们要辩证、科学地处理好政务公开和保密之间的关系。根据新修订的《保密法》，进一步做好定密工作，规范定密程序，准确确定密级。

会议强调，各部门要进一步做好涉密文件资料的清理和回收工作，防止涉密文件资料的丢失；广州市科技和信息化局针对亚运会期间政务网络信息安全保障工作召开了会议，要求各单位做好信息安全值守工作，从 10 月 19 日开始实行零报告制度，各部门要把信息安全作为保密工作的重中之重，做好信息保密工作。在亚运会即将召开之际，大家要把保密这个弦绷得更紧，切实做好人大机关的保密工作。

政府之声

网络安全问题涉及多方 需要政府介入支持

来源：ZDNET 至顶网

爱沙尼亚和新加坡的政府官员呼吁在网络安全的问题上进行有计划而周密的协作，这是涉及到每一个国家的相关利益以及在全球范围内打击狡猾的网络恐怖分子。

根据新加坡当地政府官员的说法，关于应对恶意攻击的网络安全问题必须涉及多方相关利益者，并有适当的法律框架的支持。

在周二举行的网络安全区域协作会议上，分享了 2007 年 5 月在爱沙尼亚一场规模空前黑客攻击波中的一些经验教训。

Jaak Aaviksoo 指出这一次由一个黑客组织主动的，有组织的和有针对性的网络攻击。

“如今考虑到每个国家都在使用网络，因此每个国家，每个民族都会受到黑客攻击。原则上，你可以拔掉互联网，但是关闭虚拟世界的后果可能比大网络威胁本身还要大，”他说。

2007 年，爱沙尼亚，拒绝服务攻击影响到许多公共服务，包括政府和银行。根据 Aaviksoo 表示，波罗的海国家中，每三个人中就有一人受到影响。他指出，不仅如此，人们感到此次袭击变成一个很大的问题以及“最重要的是在人们的心中的影响”。

为了更好地加强防御，各国需要设立一个“一致的”国家网络防御系统，涉及各种政府机构以及那些具有重要信息基础设施的私营部门，他说。

只有各方之间对这种合作建立相当程度的信任才会成功，他指出。

全球合作的需要

此外，国际间的合作也是至关重要的，Aaviksoo 说，他在 2007 年的网络攻击事件中努力做出应有的反应。

他说，2007 年爱沙尼亚在受到第二和第三波网络攻击时得到来自北大西洋公约组织和其他欧盟国家专家的帮助。反过来，在与爱沙尼亚同行解决这种大规模网络攻击的合作中，他们也是受益匪浅。

他指出，不断加强的国际合作也是很重要的，特别是在法律框架下对于网络攻击的处理提供支持。

“同时分析网络的攻击以及防御手段，我们非常清楚地了解，能够采取有效行动的法律工具并不到位，因为并没有一个国家或组织具有这样的法律，” Aaviksoo 说，“法律工具的缺乏对于有效的防御是一个严重的障碍，同时还要考虑到在国际间造成第三方损害的可能性，例如，当你关闭某一沟通渠道。”

各国对于规划的防御以及反击的法律框架的建立也是必要的，他指出。

Aaviksoo 补充说，此外，互联网用户必须意识到他们在预防网络攻击中所发挥的作用。

虽然可能没有必要实行诸如枪支管制法，但是当他的武器使用不当时，使用者可以被起诉，个人需要了解他们自己计算机存在着潜在威胁。

“我不认为我们可以移到一个更安全的网络空间，除非我们增加世界上所有的电脑用户对网络安全意识，”他说。

新加坡的公务员首长 Peter Ho，在周二的会议讲话中，也督促用加强协作的办法来解决网络威胁。

他指出网络安全产生了一种“不对称的局面”，作为捍卫者不得不部署比攻击者更多的资源去堵塞安全漏洞。最重要的是，黑客也正联手合作以创造更多的及更复杂的恶意软件。

因此，对于防御的捍卫者来说，协作是一次难得的重要的机会。“这需要一个网络来防御另一个网络，” Ho 说。

全球网络协议草案出炉

来源: cnbeta

据英国《每日电讯报》9月20日报道,于上周在立陶宛举行的国际互联网管理论坛上,欧洲委员会提交了一份全球“网络协议”草案,阐述了包括执行公开标准、支持网络中立、表达自由等12条“互联网管理原则”,使互联网免受政治干涉。这个互联网草案被比作1967年签署的全球《太空协定》。

这份“网络协议”将要求所有国家,支持形成互联网的技术基础,而公开和互用性则为成为网络管理协议的12条原则之二。草案还称:“网络的基础功能和核心原则必须受到保护,并以保证其基础设施、服务以及内容的网络互用性为目的,端到端原则应该在全球受到保护。”

网络用户在使用 YouTube 和 iplayer 时可能受到管制,各国政府可以跨越国界确认网络用户的身份和地址,避免网络受到可能的网络攻击或者出现网络恐怖主义。此外,这份协议还支持自由表达和自由联合的权利、网络中立原则,所有网络交易都会受到平等对待。

欧洲委员会资深官员艾尔凡纳-泰奇(音译)说,协议将要求各国政府共享网络安全信息,并且采取合理措施鼓励私营部门也如此做。但是这不包括强迫公司分享其数据安全信息。全球各国应在保护关键互联网设施方面进行合作。

这份提案是欧洲委员会出台的,这个组织总部位于法国斯特拉斯堡,共有47个成员国,致力于促进欧洲的人权、法律以及民主。网络行业的资深人士日益担忧,政府正对网络形成威胁,以将其纳入政治控制之下。牛津互联网研究所主任威廉-杜顿说,英国国会下议院近日通过的、允许版权所有者要求对非法盗版下载用户实施“警告-断网”惩罚的《数字经济法案》,就是政府单方面管理和监管互联网的最好例证。他说,每个人都担心国家政府对互联网施加影响。

苏黎世大学法律学教授、草案起草团队成员洛尔夫-韦伯说,这份网络协议堪比1967年签署的“太空协议”,那份协议规定,外太空的探索必须以所有国家的名义进行。太空探索不该存在歧视,应在平等的基础上进行,各个国家有权自由进出天体领域。

美信息安全战略跨入 3.0 时代

来源：东方网-文汇报

9月15日，在布鲁塞尔北约总部，美国国防部副部长威廉·林恩三世指出，北约盟国应该建立一个与跨大西洋联盟相重合的“网络盾牌”，并将这一“数字盾牌”和自冷战时期沿袭下来的北约“核盾牌”相提并论。这可以看作是冷战后美国信息安全战略进入第三个发展阶段的重要标识之一，预示着一一种全新的信息战略：基于“有效保护”和“大规模报复”的“积极防御”战略。

2011年11月举行的北约里斯本峰会上，预计“网络盾牌”会浮出水面。

美中央司令部内网遭“袭”

2007年至2008年间，随着美国本土面临恐怖袭击威胁的持续下降以及对布什政府以“反恐”为名过度强化信息监控感到不满等综合因素的共同作用，以国家安全局、国防部、国务院、国土安全部等为代表，美国国内重新开始了一轮对信息安全的评估。

就在同一时期，2008年一台在中东使用的美军军用笔记本电脑因某种原因接触了一个被植入木马程序的U盘，该木马程序借助这台笔记本攻入了美国中央司令部的内部军事网络。该事件被发现后对美军造成了巨大的冲击，国防部发起了名为“杨基捉虫”的行动，力求全面消除该木马间谍程序留下的隐患。一些蛛丝马迹显示，这并非恐怖分子所为，而是出自外国，很可能是俄罗斯情报机构的手笔。这一事件，加上2009年前后所谓黑客袭击谷歌服务器的事件，使得美国国防部认为其面临的主要威胁从恐怖分子转变为“有外国政府资助的黑客”，因此需要提出新的战略进行应对。

或触发网络空间“新冷战”

今年8月至9月，国防部副部长林恩先后在《华盛顿邮报》、《外交》等媒体上接受采访、撰写文章，先是详细披露了2008年美国中央司令部遭受的攻击，再系统阐述了“保障新的空间”战略的初步内容：使用“威慑”与“大规模报复”的思路，借助网络司令部自2010年10月1日起实施“积极防御”。这里的积极防御，意味着3个层面的含义：

首先，网络司令部乃至美国国防部必须确保美国及其盟国国内军用和民用网络的关键基础设施能够抵御对手发动的“突然袭击”，整个系统不应该存在某些易于被渗透的短板，此次林恩在北约提出“数字盾牌”的倡议，应该就是服务于此种考虑。

其次，美国及其盟国必须利用自身在“信息技术领域的压倒性优势”，推动政府部门与私营公司在信息安全领域的合作。林恩认为，国防部与私营公司之间的“公私”合作，将有助于美国政府利用私营公司的强大技术能力、社会网络影响，为美国及其盟国的国家安全服务。

第三，美国网络司令部乃至其盟国必须发展出有效的探测、监控、攻击的能力。自美军网络司令部成立开始，“跨境先发制人”也在积极讨论之中。所谓“跨境先发制人”，即在侦测到对方某些计算机里有针对美国的间谍软件时主动出击，入侵删除之；以及以瘫痪对方关键信息基础设施为筹码，威慑并遏制对方可能对美国及其盟国发动的攻击。

对此,《华盛顿邮报》专栏编辑戴维·伊格内修斯撰文称林恩的设想,在五角大楼内部被称为“网络战略 3.0”,以期与此前分别以“消极防御”和“控制”信息流动为特色的两种信息战略相区别。有分析者指出,3.0 版的信息战略,可能触发 21 世纪于网络空间出现的“新冷战”。

沈逸(作者为复旦大学国际关系与公共事务学院博士)

信息战略 1.0 版:对美国来说,信息安全战略的发展与演进,如同二战后的核战略,伴随着美国自身力量的变化。1998 年 5 月 22 日,克林顿政府颁布的第 63 号总统行政命令,“保护至关重要的信息基础设施”,可以看作是信息战略 1.0 版。

信息战略 2.0 版:“9·11”恐怖袭击之后,布什政府于 2003 年发布《保障信息空间安全的国家战略》,认为美国面临的主要威胁是信息技术与恐怖分子的结合,因此必须更加积极采取行动,“监控”网络信息流动以及个体使用网络的行为,在 2006 年《国际安全事务杂志》一篇专家文章将布什政府的信息战略定义为信息战略 2.0。

捷克为保护公众隐私拒绝谷歌 Street View 申请

来源:赛迪网

9 月 24 日消息,据国外媒体报道,捷克政府表示,出于保护民众个人隐私,已拒绝了谷歌扩展“Street View”的申请。

谷歌在一份声明中表示正私下里与捷克政府进行合作,并向隐私保护机构提供了所有的详细资料,以说服政府同意继续扩展“Street View”。

但捷克政府办公室官员 Igor Nemec 表示,谷歌收集数据时所用到的技术侵犯了居民的隐私。隐私保护机构已经收到了多起市民投诉,其中一人表示其住所正处于窃贼的监控之下。同时 Nemec 表示,作为一家美国公司,谷歌并没有在捷克境内设定法定代理人来处理收集到的私人数据。

谷歌“Street View”摄像车在过去几年一直错误地收集了 Wi-Fi 网络上无密码保护的有效载荷数据,从而失去了许多欧洲国家的信任。

谷歌方面表示,在问题解决之前,不会在捷克采集新的数据,但以前拍摄的布拉格和其他城市街景照片仍可以看到。

国家标准化管理委员会批准 18 项信息安全标准

来源：中国计算机安全

由全国信息安全标准化技术委员会组织制定的《公钥基础设施安全支撑平台技术框架》、《证书认证系统密码及其相关安全技术规范》、《信息系统安全等级保护 实施指南》等 18 项信息安全技术标准，近日经国家标准化管理委员会批准发布，并将于 2011 年 2 月 1 日起实施。这批标准的发布实施，对于完善我国信息安全 标准体系，规范和指导我国信息安全保障体系建设具有重要意义。

附件：18 项信息安全国家标准清单

序号	标准编号	标准名称	实施日期
1	GB/T 25055-2010	信息安全技术 公钥基础设施安全支撑平台技术框架	2011. 02. 01
2	GB/T 25056-2010	信息安全技术 证书认证系统密码及其相关安全技术规范	2011. 02. 01
3	GB/T 25057-2010	信息安全技术 公钥基础设施 电子签名卡应用接口基本要求	2011. 02. 01
4	GB/T 25058-2010	信息安全技术 信息系统安全等级保护实施指南	2011. 02. 01
5	GB/T 25059-2010	信息安全技术 公钥基础设施 简易在线证书状态协议	2011. 02. 01
6	GB/T 25060-2010	信息安全技术 公钥基础设施 X.509 数字证书应用接口规范	2011. 02. 01
7	GB/T 25061-2010	信息安全技术 公钥基础设施 XML 数字签名语法与处理规范	2011. 02. 01

8	GB/T 25062-2010	信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范	2011.02.01
9	GB/T 25063-2010	信息安全技术 服务器安全测评要求	2011.02.01
10	GB/T 25064-2010	信息安全技术 公钥基础设施 电子签名格式规范	2011.02.01
11	GB/T 25065-2010	信息安全技术 公钥基础设施 签名生成应用程序的安全要求	2011.02.01
12	GB/T 25066-2010	信息安全技术 信息安全产品类别与代码	2011.02.01
13	GB/T 25067-2010	信息技术 安全技术 信息安全管理体系 审核认证机构的要求	2011.02.01
14	GB/T 25069-2010	信息安全技术 术语	2011.02.01
15	GB/T 25070-2010	信息安全技术 信息系统等级保护安全设计技术要求	2011.02.01
16	GB/T 25068.3-2010	信息技术 安全技术 IT 网络安全 第3部分：使用安全网关的网间通信安全保护	2011.02.01
17	GB/T 25068.4-2010	信息技术 安全技术 IT 网络安全 第4部分：远程接入的安全保护	2011.02.01
18	GB/T 25068.5-2010	信息技术 安全技术 IT 网络安全 第5部分：使用虚拟专用网的	2011.02.01

		跨网通信安全保护	
--	--	----------	--

病毒播报

Linux 内核中的漏洞提供了非法根权限

来源：safebeta

当前（以及任何早期）64 位系统 Linux 在 32 位兼容模式下有一处漏洞，可以用来增强用户权限。举例说，来袭者可以闯入系统，利用 Web 服务器的一处漏洞获取受害系统的完全根权限（或称超级权限）或准入许可。

据报道，问题出自 32 位的调用模拟层没有验证调用是否存在于系统调用表中。发现这一问题的 Ben Hawkes 说，这一隐患可以被用来以内核权限执行任意代码。目前已经有一个利用该漏洞的方法（可直接以源码形式下载）流通；在一个由 The H 的合作者在 64 位 Ubuntu 10.04 上实行的测试当中，它以根权限打开了一个 shell。

内核开发者已经在软件仓库纠正了这一瑕疵，Linux 的发行厂商们很可能近期会推出新的内核来关闭这一漏洞。那之前，如果你不必要这一功能的话，关闭 32 位 ELF 支持以解决这一问题。具体命令见：“应对 Ac1db1tch3z 漏洞”。

Hawkes 说，早在 2007 年，这一漏洞就被发现并被纠正了。但是在 2008 年的某个点上，开发者明显移除了那一补丁，再引入了漏洞。以前的入侵只需稍加改变就可以用在新的漏洞上。

报告称 Facebook 是最危险社交网站

来源：新浪

北京时间 9 月 19 日早间消息，据国外媒体报道，互联网安全公司熊猫公司(Panda)近日公布的一份报告显示，约 1/3 的美国中小型企业因访问 Facebook 等社交网站而被计算机病毒感染。

熊猫公司今年 7 月对 315 名中小型企业员工进行了调查，发现这些企业基本上不太限制员工对社交网站的访问。报告显示，69.3%的企业访问 Facebook，44.4%访问 Twitter，32%访问 YouTube，22.9%访问 LinkedIn。

在访问社交网站的企业中，38.2%表示工作效率受到影响，33.3%被恶意软件感染，23%遭到隐私侵犯，18.6%表示影响公司网络资源。

在隐私侵犯一项中，抱怨 Facebook 的比例高达 73.2%，Twitter 为 50.7%，YouTube 为 29.6%，LinkedIn 为 16.9%。在恶意软件方面，Facebook 所占比例仍最高，为 71.6%。

中秋期间上网需防范间谍木马病毒窃密

来源：新华网

上海 9 月 19 日电（记者陆文军）即将到来的中秋佳节，人们在享受上网休闲娱乐的同时，切不可对网络病毒掉以轻心。上海计算机病毒防范服务中心监控发现，几种危险间谍木马病毒将在中秋节假日期间集中爆发，这些黑客病毒不但能够完全控制主机，而且还可能窃取用户私人信息，须倍加防范。

据介绍，近期将有多种间谍木马病毒在网上集中爆发，如“砸波变种”“霸族变种”“黑孔变种”等，这些病毒一旦侵入用户电脑，会在被感染系统的后台连接黑客指定的远程站点，然后侦听黑客的指令，从而达到远程控制的目的。黑客会通过病毒监视被感染系统用户的键盘输入、屏幕显示、光驱操作、文件读写、鼠标操作和摄像头操作等，还可以窃取、修改或删除用户计算机中存储的机密信息，从而对用户的信息安全、个人隐私构成严重的威胁。

反病毒专家建议，节日期间电脑用户也不要忘记对安全软件及时升级，做好“漏洞扫描与修复”，打好补丁，弥补系统漏洞；尤其要注意不浏览不良网站，不随意下载安装可疑插件，不接收可疑文件，防范此类黑客病毒。

Adobe 发布补丁修复 Flash 播放器漏洞

来源：比特网 ChinaByte

Adobe 刚刚发布了一个补丁来修复 Flash Player 10.1.82.76 以及更早版本中的漏洞，该漏洞影响 Windows, Macintosh, Linux, Solaris，并受此影响 Android，并且攻击代码已经出现。

更有趣的是，这个漏洞同时还影响功能不同的软件 Adobe Redaer，照例也是全平台中招，因此希望机子上有相关软件的用户尽快安装补丁以避免风险。

超级病毒疑似攻击伊朗核电站 疑是国家行为

来源：cnbeta

据英国《每日邮报》9 月 25 日（北京时间）报道，日前，世界上首个网络“超级武器”，一种名为 Stuxnet 的计算机病毒已经感染了全球超过 45000 个网络，伊朗遭到的攻击最为严重，60% 的个人电脑感染了这种病毒。计算机安防专家认为，该病毒是有史以来最高端的“蠕虫”病毒，其目的可能是要攻击伊朗的布什尔核电站。布什尔核电站目前正在装备核燃料，按照计划，它本应在今年 8 月开始运行。

“蠕虫”是一种典型的计算机病毒，它能自我复制，并将副本通过网络传输，任何一台个人电脑只要和染毒电脑相连，就会被感染。这种 Stuxnet 病毒于今年 6 月首次被检测出来，是第一个专门攻击真实世界中基础设施的“蠕虫”病毒，比如发电站和水厂。目前互联网安全专家对此表示担心。

一些专家认为，Stuxnet 病毒是专门设计来攻击伊朗重要工业设施的，包括上个月竣工的布什尔核电站。它在入侵一台个人电脑后，会寻找广泛用于控制工业系统如工厂、发电站自动运行的一种西门子软件。它通过对软件重新编程实施攻击，给机器编一个新程序，或输入潜伏极大风险的指令。专家指出，病毒能控制关键过程并开启一连串执行程序，最终导致整个系统自我毁灭。

卡巴斯基的高级安防研究员戴维·爱姆说，Stuxnet 与其它病毒的不同之处，就在于它瞄准的是现实世界。他们公司已经和微软联手，查找程序中的编码漏洞，防止新病毒找到它。

爱姆说，通常的大部分病毒像个大口径短枪到处开火，而 Stuxnet 像个狙击手，只瞄准特定的系统。一旦它们发现了编码缺陷，就好比找到了房子上的天窗，然后用一把羊头镐撬开一个更大的洞。Stuxnet 被设计出来，纯粹就是为了搞破坏。

德国网络安全研究员拉尔夫·朗纳已经破解了 Stuxnet 的编码，并将之公布于众。他坚信 Stuxnet 被设计出来，就是为了寻找基础设施并破坏其关键部分。他说，这是一种百分之百直接面向现实世界中工业程序的网络攻击。它绝非所谓的间谍病毒，而是纯粹的破坏病毒。

朗纳说，Stuxnet 病毒的高端性，意味着只有一个“国家”才能把它开发出来。根据我们所掌握

的计算机法医方面证据，它的意图很明显，就是执行破坏性攻击，毁掉大量的内部信息。这并非某个坐在父母家里的地下室里的骇客能干得出来的，这种攻击的来源指向的是一个国家。Stuxnet 很可能已经攻击了它的目标，只不过我们还没有接到消息而已。

订机票慎防航空公司“山寨网”

来源：大洋网-信息时报

“从航空公司官方网站找到的电话怎么可能是骗子呢？”昨日，有旅客在网站上订了从广州飞往南京的机票，不料却被骗了。双节来临，机票价格也突飞猛涨，折扣票吸引了大部分出游市民的眼球，但折扣票很有可能就是“陷阱”。

航空公司表示，市民在订票的时候要到正规的网站，不要看折扣低就预订。

要汇款到指定账号多半是假冒代理

宋小姐告诉记者，她前几日在“南航”的网站看到飞往南京的机票有折扣，大概 800 元左右。宋小姐通过这个网站预付机票钱，这时就有工作人员提醒，为防止机票价格上涨，要在两个小时之内把机票钱汇到指定的账户里面。宋小姐担心机票涨价便赶紧汇钱过去，但是昨日宋小姐想确认航班起飞时间的时候，却被告知没有她的名字。这时她才恍然大悟，被所谓的山寨网站欺骗了。

“最近我们接到消费者投诉，网上出现了一些与各航空公司官方网站规划以及内容极为相似的‘山寨’网站，很容易被顾客误认为是某航空公司的正规网站。”携程网的业务总监邵季红表示。

旅游业人士称，让顾客用银行卡直接汇到银行账户的多半是假冒代理，消费者一定要提高警惕，尽量选择知名代理商渠道购票。

400 开头的电话也可能是骗子

据称，一些不法分子往往通过旅游搜索引擎或购物平台发布廉价机票信息，引诱订票者上钩，进行诈骗，而很多不法分子为掩人耳目，让消费者放松警惕，往往也采用 400 开头的客服电话，当消费者拨打该 400 电话，汇款过去之后却拿不到机票。

除了电话有假，还有不少消费者遇到过订机票拿到假行程单的情况。

据了解，这种情况一般是由于一些黑票代通过低价高开或出售假机票等情况引起。基本是在假行程单上修改了真实机票的价格，如代理点购买的是三折机票，却开出全价机票收取客人全价费用，一旦客人要求更改行程的话，便有可能遭遇到低价票无法改签等问题。另外，还有黑票代用假行程单蒙骗消费者，而实际上根本没订票或已经退票，也将导致顾客无法登机。

邵季红表示，不要被旅游搜索引擎搜到的 400 开头的所谓企业客服专用号联系电话蒙蔽，查询到 400 的电话最好通过搜索引擎反查信息是否有不一致的地方，消费者在订票时也应尽量找官网购买机票。

专家支招

招辨识机票真伪

1. 正规渠道购票。购买飞机票一定要到正规销售代理商或航空公司直属售票处、网站等。
2. 及时查验电子客票行程单真伪。消费者在拿到行程单后，可以检查行程单右上角印刷序号的后 4 位是否与验证码一致，是否有 SW、MH 字样的水印，行程单复印后，会在复印件的黄条位置上显现出“复印无效”的字样。消费者还可以拨打中航信机票服务热线 4008158888 或者登录中航信网站 www.travelsky.com 进行验证。
3. 核对机票信息是否有误。仔细核对行程单上显示的名字、航班日期、航程、直飞或中转航班信息、客票的有效期与限制条件等。网上支付获取电子客票号的也应仔细核对相关信息。
4. 国际飞机票报销还需索取商业发票。电子客票行程单可作报销凭证，国际航班报销则应索要正规商业发票。

瑞星称 Stuxnet 病毒全球肆虐

来源：新浪

9 月 25 日下午消息，瑞星公司宣布监测到一个席卷全球工业界的病毒已经入侵我国，这种名为 Stuxnet 的蠕虫病毒已经造成伊朗核电站推迟发电，目前国内已有近 500 万网民、及多个行业的领军企业遭此病毒攻击。瑞星反病毒专家警告说，我们许多大型重要企业在安全制度上存在缺失，可能促进 Stuxnet 病毒在企业中的大规模传播。

瑞星专家表示，这是世界上首个专门针对工业控制系统编写的破坏性病毒，它同时利用包括 MS10-046、MS10-061、MS08-067 等 7 个最新漏洞进行攻击。这 7 个漏洞中，有 5 个是针对 windows 系统，2 个是针对西门子 SIMATIC WinCC 系统。另外在关于微软的 5 个漏洞中，目前有两个本地提权漏洞仍未修复。

该病毒通过伪装 RealTek 与 JMicron 两大公司的数字签名，从而顺利绕过安全产品的检测。从编写手法上看，该病毒还有很大的改进余地，将来很可能出现同样原理的复杂病毒。

据瑞星技术部门分析，Stuxnet 病毒专门针对西门子公司 SIMATIC WinCC 监控与数据采集 (SCADA) 系统进行攻击，由于该系统在我国的多个重要行业应用广泛，被用来进行钢铁、电力、能源、化工等重要行业的人机交互与监控，一旦攻击成功，则可能造成使用这些企业运行异常，甚至造成商业资料失窃、停工停产等严重事故。

该病毒主要通过 U 盘和局域网进行传播，由于安装 SIMATIC WinCC 系统的电脑一般会与互联网物理隔绝，因此黑客特意强化了病毒的 U 盘传播能力。如果企业没有针对 U 盘等可移动设备进行严格管理，导致有人在局域网内使用了带毒 U 盘，则整个网络都会被感染。

Stuxnet 病毒被多国安全专家形容为全球首个“超级工厂病毒”。截至目前，Stuxnet 病毒已经感染了全球超过 45000 个网络，伊朗、印尼、美国、台湾等多地均不能幸免，其中，以伊朗遭到的攻击最为严重，60% 的个人电脑感染了这种病毒。

瑞星安全专家提醒广大政府及企业级用户：一定要严格限制 U 盘在密级网络中的应用，如果必须使用的，则应该建立使用登记和责任追究制度。另外，瑞星杀毒软件网络版也针对此病毒，提供了完善的 U 盘病毒预防、网络内安全管理、恶性病毒扫描等全套解决方案。

QQ 为推产品谎报漏洞

来源：金羊网

2 年前，一位名叫 NeoN 的俄罗斯黑客被各国媒体争相报道，原因是他做出了一种专门恐吓用户电脑“中毒”的流氓软件，威胁用户购买价格 49.95 美元的某款杀毒软件。如今，国内知名互联网公司 QQ 似乎也已经被黑客 NeoN “附体”，竟然开始用“检测到高危漏洞”欺骗、恐吓用户，以此方式来推广 QQ 电脑管家。

不同的是，黑客 NeoN 专门攻击美国网民，从不向自己俄罗斯同胞的电脑下手，而 QQ 的“高危漏洞”提示则是针对 QQ 用户进行弹窗通知，恐吓用户下载安装 QQ 电脑管家。很多网友在按照提示去修复所谓的“高危漏洞”时才发现，这不过是一些可选的功能性补丁，和电脑系统安全并无关系，部分网友甚至还因此打上了 Windows 操作系统的正版验证补丁。

据国内知名安全论坛卡饭的网友 baibao578 反馈，他的电脑仅安装了 QQ2010 SP1 精简版，最近却突然弹窗提示说“您的系统存在 3 各高危漏洞。系统存在严重风险，易导致 QQ 密码被木马盗取，请尽快使用 QQ 电脑管家修复”。让卡饭网友惊诧的是，QQ 只是一款聊天工具，并没有漏洞检测功能，它又是如何发现用户电脑上的“高危漏洞”呢？

原来，QQ 电脑管家的前身就是 QQ 医生。早在今年春节期间，腾讯在国内大量中小城市的 QQ 用户电脑上大规模强制安装 QQ 医生，如果拒绝安装则无法登陆 QQ。此后由于这款软件并不好用，经常误打补丁导致用户电脑故障，QQ 医生已经被用户卸载得几近销声匿迹。这次腾讯卷土重来，不光给 QQ2010 的用户偷偷捆绑安装“改头换面”的 QQ 电脑管家，还用上了谎报漏洞的方式。

据悉，在 QQ 电脑管家的恐吓式营销之前，国内曾有一家名为“安铁诺”的软件学习了黑客 NeoN 的伎俩。该软件利用木马进行推广，威胁中招用户电脑“因感染超强木马将高温爆炸”，并且把用户导向一个带有“系统瘫痪倒计时”的销售页面，以 10 元/月的资费出售安铁诺“系统优化安全专家”序列号。

有网友评论说，腾讯之所以不惜公然欺骗、恐吓用户，强行推广安装 QQ 电脑管家，很可能是急于在 QQ 用户中部署一款自己的安全软件，便于查杀各种修改版的 QQ 和游戏外挂。毕竟，DNF

等腾讯游戏和 QQ 会员服务才是腾讯公司收入的主要来源。

安全漏洞发现情况周报表

(09 月 20 日至 09 月 26 日)

上报单位：国家计算机网络入侵防范中心

上报时间： 2010 年 09 月 27 日

监测情况	本周共收集和整理安全漏洞 77 个，其中高危漏洞 20 个，中等威胁漏 47 个，低威胁漏洞 10 个。漏洞总量与上周相比有所下降，其中高危漏洞是上周的 48.78%，中等威胁漏洞是上周的 1.04 倍，低威胁漏洞是上周的 2.5 倍。
安全形势分析	本周 Adobe 发布了一个补丁程序来修复 Flash Player 10.1.82.76 以及更早版本中的一个任意代码执行漏洞，针对该漏洞的攻击代码已经出现，建议用户尽快下载补丁程序，保证系统安全。 另外，Linux Kernel 存在一个 32 位系统调用模拟层内核权限提升漏洞，攻击者成功利用该漏洞可以提升本地权限，希望用户关注厂商官网，及时下载更新或补丁程序。此外，Cisco IOS 修复了多个拒绝服务漏洞。 综合分析，本周安全漏洞威胁程度为中度偏下。

基本情况	发现安全漏洞数量				高危漏洞数量				“零日”漏洞数量	
	77				20				0	
5 大安全漏洞	排名	名称	CVE 编号	类型	危险等级	漏洞起因	受影响的系统/软件	可能发生的攻击及危害	被利用情况	补丁及控制策略
	1	Linux kernel 本地权限提升漏洞	CVE-2010-3301	设计错误	高	系统初始设计有误	详见附表	攻击者成功利用该漏洞可以获得提升本地权限。	未知	安全公告及厂商补丁： http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=eefdca043e8391dcd719711716492063030b55ac

	2	Cisco IOS SSL VPN 拒绝 服务 漏洞	CVE-2010 -2836	资 源 管 理 错 误; ;	高	没有正确 管理系统 资源	详见附 表	攻击者成 功利用该 漏洞可能 引起拒绝 服务（内 存破坏）。	未知	安全公告及厂商补丁： http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a312.shtml
	3	Cisco IOS 及 Unifi ed Commu nicat ion Manag er 多 个拒 绝服 务漏 洞	CVE-2010 -2834 CVE-2010 -2835	未 知	高	未知	详见附 表	攻击者成 功利用该 漏洞可能 引起拒绝 服务（设 备重启或 语言服务 停止）。	未知	安全公告及厂商补丁： http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a30f.shtml
	4	Cisco IOS 多 个 网 络 地 址 转 换 漏洞	CVE-2010 -2831 CVE-2010 -2832 CVE-2010 -2833	未 知	高	未知	详见附 表	攻击者成 功利用该 漏洞可能 引起拒绝 服务（设 备重启）。	未知	安全公告及厂商补丁： http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a311.shtml

	5	Cisco IOS H. 323 多个 拒绝 服务 漏洞	CVE-2010 -2828 CVE-2010 -2829	未 知	高	未知	详见附 表	攻击者成功利用该漏洞可能引起拒绝服务（设备重启）。	未知	安全公告及厂商补丁： http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a300.shtml
--	---	--	--	--------	---	----	----------	---------------------------	----	---

附表:

排名	名称	受影响的系统/软件
1	Linux kernel 本地 权限提升漏洞	linux, kernel, 2. 6. 21. 6; linux, kernel, 2. 6. 21. 3; linux, kernel, 2. 6. 21. 7; linux, kernel, 2. 6. 21. 5; linux, kernel, 2. 6. 21; linux, kernel, 2. 6. 21. 1; linux, kernel, 2. 6. 21. 2; linux, kernel, 2. 6. 20. 3; linux, kernel, 2. 6. 20. 16; linux, kernel, 2. 6. 20. 4; linux, kernel, 2. 6. 20. 5; linux, kernel, 2. 6. 20. 6; linux, kernel, 2. 6. 20. 7; linux, kernel, 2. 6. 20. 8; linux, kernel, 2. 6. 20. 9; linux, kernel, 2. 6. 20. 10; linux, kernel, 2. 6. 20. 11; linux, kernel, 2. 6. 20. 12; linux, kernel, 2. 6. 20. 13; linux, kernel, 2. 6. 20. 14; linux, kernel, 2. 6. 20. 15; linux, kernel, 2. 6. 20. 21; linux, kernel, 2. 6. 20. 18; linux, kernel, 2. 6. 20; linux, kernel, 2. 6. 20. 17; linux, kernel, 2. 6. 20. 2; linux, kernel, 2. 6. 20. 20; linux, kernel, 2. 6. 20. 19; linux, kernel, 2. 6. 20. 1;

	linux, kernel, 2. 6. 19. 7; linux, kernel, 2. 6. 19. 5; linux, kernel, 2. 6. 19. 6; linux, kernel, 2. 6. 19. 4; linux, kernel, 2. 6. 19; linux, kernel, 2. 6. 19. 2; linux, kernel, 2. 6. 19. 1; linux, kernel, 2. 6. 19. 3; linux, kernel, 2. 6. 18, rc5; linux, kernel, 2. 6. 18, rc6; linux, kernel, 2. 6. 18, rc7; linux, kernel, 2. 6. 18, rc1; linux, kernel, 2. 6. 18, rc2; linux, kernel, 2. 6. 18, rc3; linux, kernel, 2. 6. 18, rc4; linux, kernel, 2. 6. 18. 1; linux, kernel, 2. 6. 18; linux, kernel, 2. 6. 18. 3; linux, kernel, 2. 6. 18. 2; linux, kernel, 2. 6. 18. 5; linux, kernel, 2. 6. 18. 4; linux, kernel, 2. 6. 18. 7; linux, kernel, 2. 6. 18. 6; linux, kernel, 2. 6. 18. 8; linux, kernel, 2. 6. 17. 4; linux, kernel, 2. 6. 17. 5; linux, kernel, 2. 6. 17. 2; linux, kernel, 2. 6. 17. 3; linux, kernel, 2. 6. 17; linux, kernel, 2. 6. 17. 1; linux, kernel, 2. 6. 17. 12; linux, kernel, 2. 6. 17. 13; linux, kernel, 2. 6. 17. 10;
--	---

	linux, kernel, 2. 6. 17. 11; linux, kernel, 2. 6. 17. 8; linux, kernel, 2. 6. 17. 9; linux, kernel, 2. 6. 17. 6; linux, kernel, 2. 6. 17. 7; linux, kernel, 2. 6. 17. 14; linux, kernel, 2. 6. 16. 8; linux, kernel, 2. 6. 16. 7; linux, kernel, 2. 6. 16. 6; linux, kernel, 2. 6. 16. 5; linux, kernel, 2. 6. 16. 12; linux, kernel, 2. 6. 16. 11; linux, kernel, 2. 6. 16. 10; linux, kernel, 2. 6. 16. 9; linux, kernel, 2. 6. 16; linux, kernel, 2. 6. 16. 4; linux, kernel, 2. 6. 16. 3; linux, kernel, 2. 6. 16. 2; linux, kernel, 2. 6. 16. 1; linux, kernel, 2. 6. 16. 61; linux, kernel, 2. 6. 16. 62; linux, kernel, 2. 6. 16. 52; linux, kernel, 2. 6. 16. 51; linux, kernel, 2. 6. 16. 50; linux, kernel, 2. 6. 16. 49; linux, kernel, 2. 6. 16. 48; linux, kernel, 2. 6. 16. 47; linux, kernel, 2. 6. 16. 46; linux, kernel, 2. 6. 16. 45; linux, kernel, 2. 6. 16. 60; linux, kernel, 2. 6. 16. 59; linux, kernel, 2. 6. 16. 58; linux, kernel, 2. 6. 16. 57;
--	---

	linux, kernel, 2. 6. 16. 56; linux, kernel, 2. 6. 16. 55; linux, kernel, 2. 6. 16. 54; linux, kernel, 2. 6. 16. 53; linux, kernel, 2. 6. 16. 33; linux, kernel, 2. 6. 16. 34; linux, kernel, 2. 6. 16. 35; linux, kernel, 2. 6. 16. 36; linux, kernel, 2. 6. 16. 29; linux, kernel, 2. 6. 16. 30; linux, kernel, 2. 6. 16. 31; linux, kernel, 2. 6. 16. 32; linux, kernel, 2. 6. 16. 41; linux, kernel, 2. 6. 16. 42; linux, kernel, 2. 6. 16. 43; linux, kernel, 2. 6. 16. 44; linux, kernel, 2. 6. 16. 37; linux, kernel, 2. 6. 16. 38; linux, kernel, 2. 6. 16. 39; linux, kernel, 2. 6. 16. 40; linux, kernel, 2. 6. 16. 18; linux, kernel, 2. 6. 16. 31, -rc1; linux, kernel, 2. 6. 16. 17; linux, kernel, 2. 6. 16. 31, -rc4; linux, kernel, 2. 6. 16. 20; linux, kernel, 2. 6. 16. 31, -rc2; linux, kernel, 2. 6. 16. 19; linux, kernel, 2. 6. 16. 31, -rc3; linux, kernel, 2. 6. 16. 14; linux, kernel, 2. 6. 16. 13; linux, kernel, 2. 6. 16. 16; linux, kernel, 2. 6. 16. 15; linux, kernel, 2. 6. 16. 26;
--	--

	linux, kernel, 2. 6. 16. 25; linux, kernel, 2. 6. 16. 28; linux, kernel, 2. 6. 16. 27; linux, kernel, 2. 6. 16. 22; linux, kernel, 2. 6. 16. 21; linux, kernel, 2. 6. 16. 24; linux, kernel, 2. 6. 16. 23; linux, kernel, 2. 6. 16. 31, -rc5; linux, kernel, 2. 6. 15. 7; linux, kernel, 2. 6. 15. 6; linux, kernel, 2. 6. 15. 5; linux, kernel, 2. 6. 15; linux, kernel, 2. 6. 15. 3; linux, kernel, 2. 6. 15. 4; linux, kernel, 2. 6. 15. 1; linux, kernel, 2. 6. 15. 2; linux, kernel, 2. 6. 14. 7; linux, kernel, 2. 6. 14. 5; linux, kernel, 2. 6. 14. 6; linux, kernel, 2. 6. 14; linux, kernel, 2. 6. 14. 3; linux, kernel, 2. 6. 14. 4; linux, kernel, 2. 6. 14. 1; linux, kernel, 2. 6. 14. 2; linux, kernel, 2. 6. 13. 5; linux, kernel, 2. 6. 13. 3; linux, kernel, 2. 6. 13. 4; linux, kernel, 2. 6. 13; linux, kernel, 2. 6. 13. 2; linux, kernel, 2. 6. 13. 1; linux, kernel, 2. 6. 12. 3; linux, kernel, 2. 6. 12. 2; linux, kernel, 2. 6. 12. 5;
--	--

	linux, kernel, 2. 6. 12. 4; linux, kernel, 2. 6. 12. 6; linux, kernel, 2. 6. 12. 1; linux, kernel, 2. 6. 12; linux, kernel, 2. 6. 11. 8; linux, kernel, 2. 6. 11. 7; linux, kernel, 2. 6. 11. 10; linux, kernel, 2. 6. 11. 9; linux, kernel, 2. 6. 11. 12; linux, kernel, 2. 6. 11. 11; linux, kernel, 2. 6. 11; linux, kernel, 2. 6. 11. 1; linux, kernel, 2. 6. 11. 2; linux, kernel, 2. 6. 11. 3; linux, kernel, 2. 6. 11. 4; linux, kernel, 2. 6. 11. 5; linux, kernel, 2. 6. 11. 6; linux, kernel, 2. 6. 10; linux, kernel, 2. 6. 9; linux, kernel, 2. 6. 8; linux, kernel, 2. 6. 8. 1; linux, kernel, 2. 6. 7; linux, kernel, 2. 6. 6; linux, kernel, 2. 6. 5; linux, kernel, 2. 6. 4; linux, kernel, 2. 6. 3; linux, kernel, 2. 6. 2; linux, kernel, 2. 6. 1; linux, kernel, 2. 6. 0; linux, kernel, 2. 6. 33, rc4; linux, kernel, 2. 6. 33, rc2; linux, kernel, 2. 6. 33, rc3; linux, kernel, 2. 6. 33, rc6;
--	--

	linux, kernel, 2. 6. 33, rc5; linux, kernel, 2. 6. 33, rc1; linux, kernel, 2. 6. 33, rc7; linux, kernel, 2. 6. 32, rc7; linux, kernel, 2. 6. 32, rc8; linux, kernel, 2. 6. 32, rc4; linux, kernel, 2. 6. 32, rc3; linux, kernel, 2. 6. 32, rc1; linux, kernel, 2. 6. 32, git-6; linux, kernel, 2. 6. 32. 5; linux, kernel, 2. 6. 32. 6; linux, kernel, 2. 6. 32. 7; linux, kernel, 2. 6. 32; linux, kernel, 2. 6. 32. 3; linux, kernel, 2. 6. 32. 2; linux, kernel, 2. 6. 32. 4; linux, kernel, 2. 6. 32. 1; linux, kernel, 2. 6. 32, rc6; linux, kernel, 2. 6. 32, rc5; linux, kernel, 2. 6. 31. 1; linux, kernel, 2. 6. 31. 3; linux, kernel, 2. 6. 31. 2; linux, kernel, 2. 6. 31. 4; linux, kernel, 2. 6. 31, rc6; linux, kernel, 2. 6. 31, rc5; linux, kernel, 2. 6. 31, rc4; linux, kernel, 2. 6. 31, rc3; linux, kernel, 2. 6. 31, rc1; linux, kernel, 2. 6. 31, rc2; linux, kernel, 2. 6. 31; linux, kernel, 2. 6. 31. 5; linux, kernel, 2. 6. 31. 6; linux, kernel, 2. 6. 31, rc7;
--	---

	linux, kernel, 2. 6. 31, rc8; linux, kernel, 2. 6. 33. 1; linux, kernel, 2. 6. 32. 8; linux, kernel, 2. 6. 32. 9; linux, kernel, 2. 6. 32. 10; linux, kernel, 2. 6. 31. 7; linux, kernel, 2. 6. 31. 8; linux, kernel, 2. 6. 31. 9; linux, kernel, 2. 6. 31. 10; linux, kernel, 2. 6. 31. 11; linux, kernel, 2. 6. 31. 12; linux, kernel, 2. 6. 30. 9; linux, kernel, 2. 6. 30. 4; linux, kernel, 2. 6. 30, rc3; linux, kernel, 2. 6. 30. 2; linux, kernel, 2. 6. 30. 6; linux, kernel, 2. 6. 30. 8; linux, kernel, 2. 6. 30. 7; linux, kernel, 2. 6. 30. 5; linux, kernel, 2. 6. 30. 3; linux, kernel, 2. 6. 30, rc6; linux, kernel, 2. 6. 30, rc2; linux, kernel, 2. 6. 30, rc5; linux, kernel, 2. 6. 30; linux, kernel, 2. 6. 30. 1; linux, kernel, 2. 6. 30, rc1; linux, kernel, 2. 6. 30, rc7-git6; linux, kernel, 2. 6. 30. 10; linux, kernel, 2. 6. 29. 6; linux, kernel, 2. 6. 29. 5; linux, kernel, 2. 6. 29. 4; linux, kernel, 2. 6. 29. 3; linux, kernel, 2. 6. 29. 2;
--	---

	linux, kernel, 2. 6. 29. 1; linux, kernel, 2. 6. 29; linux, kernel, 2. 6. 29, git1; linux, kernel, 2. 6. 29, rc1; linux, kernel, 2. 6. 29, rc2; linux, kernel, 2. 6. 29, rc2_git7; linux, kernel, 2. 6. 29, rc8-kk; linux, kernel, 2. 6. 28. 5; linux, kernel, 2. 6. 28, rc7; linux, kernel, 2. 6. 28. 10; linux, kernel, 2. 6. 28. 8; linux, kernel, 2. 6. 28, rc5; linux, kernel, 2. 6. 28, rc2; linux, kernel, 2. 6. 28, rc1; linux, kernel, 2. 6. 28, rc4; linux, kernel, 2. 6. 28, rc3; linux, kernel, 2. 6. 28. 9; linux, kernel, 2. 6. 28; linux, kernel, 2. 6. 28. 4; linux, kernel, 2. 6. 28. 1; linux, kernel, 2. 6. 28. 6; linux, kernel, 2. 6. 28. 7; linux, kernel, 2. 6. 28, git7; linux, kernel, 2. 6. 28, rc6; linux, kernel, 2. 6. 28. 3; linux, kernel, 2. 6. 28. 2; linux, kernel, 2. 6. 27, rc9; linux, kernel, 2. 6. 27, rc8; linux, kernel, 2. 6. 27. 20; linux, kernel, 2. 6. 27. 8; linux, kernel, 2. 6. 27. 23; linux, kernel, 2. 6. 27. 24; linux, kernel, 2. 6. 27, rc5;
--	---

	linux, kernel, 2. 6. 27, rc4; linux, kernel, 2. 6. 27, rc7; linux, kernel, 2. 6. 27, rc6; linux, kernel, 2. 6. 27, rc1; linux, kernel, 2. 6. 27, rc3; linux, kernel, 2. 6. 27, rc2; linux, kernel, 2. 6. 27. 10; linux, kernel, 2. 6. 27. 9; linux, kernel, 2. 6. 27. 12; linux, kernel, 2. 6. 27. 11; linux, kernel, 2. 6. 27. 22; linux, kernel, 2. 6. 27. 7; linux, kernel, 2. 6. 27. 34; linux, kernel, 2. 6. 27. 33; linux, kernel, 2. 6. 27. 36; linux, kernel, 2. 6. 27. 35; linux, kernel, 2. 6. 27. 37; linux, kernel, 2. 6. 27. 5; linux, kernel, 2. 6. 27. 6; linux, kernel, 2. 6. 27; linux, kernel, 2. 6. 26. 1; linux, kernel, 2. 6. 26. 3; linux, kernel, 2. 6. 26. 5; linux, kernel, 2. 6. 26. 2; linux, kernel, 2. 6. 26, rc4; linux, kernel, 2. 6. 26. 8; linux, kernel, 2. 6. 26. 7; linux, kernel, 2. 6. 26. 6; linux, kernel, 2. 6. 26. 4; linux, kernel, 2. 6. 26; linux, kernel, 2. 6. 25; linux, kernel, 2. 6. 25. 1; linux, kernel, 2. 6. 25. 10;
--	--

	linux, kernel, 2. 6. 25. 11; linux, kernel, 2. 6. 25. 12; linux, kernel, 2. 6. 25. 13; linux, kernel, 2. 6. 25. 14; linux, kernel, 2. 6. 25. 15; linux, kernel, 2. 6. 25. 16; linux, kernel, 2. 6. 25. 17; linux, kernel, 2. 6. 25. 18; linux, kernel, 2. 6. 25. 19; linux, kernel, 2. 6. 25. 2; linux, kernel, 2. 6. 25. 20; linux, kernel, 2. 6. 25. 3; linux, kernel, 2. 6. 25. 4; linux, kernel, 2. 6. 25. 5; linux, kernel, 2. 6. 25. 6; linux, kernel, 2. 6. 25. 7; linux, kernel, 2. 6. 25. 8; linux, kernel, 2. 6. 25. 9; linux, kernel, 2. 6. 24; linux, kernel, 2. 6. 24. 1; linux, kernel, 2. 6. 24. 2; linux, kernel, 2. 6. 24. 3; linux, kernel, 2. 6. 24. 4; linux, kernel, 2. 6. 24. 5; linux, kernel, 2. 6. 24. 6; linux, kernel, 2. 6. 24. 7; linux, kernel, 2. 6. 24, rc1; linux, kernel, 2. 6. 24, rc2; linux, kernel, 2. 6. 24, rc3; linux, kernel, 2. 6. 24, rc4; linux, kernel, 2. 6. 24, rc5; linux, kernel, 2. 6. 23. 15; linux, kernel, 2. 6. 23. 17;
--	--

	linux, kernel, 2. 6. 23. 16; linux, kernel, 2. 6. 23. 11; linux, kernel, 2. 6. 23. 9; linux, kernel, 2. 6. 23. 13; linux, kernel, 2. 6. 23. 12; linux, kernel, 2. 6. 23. 8; linux, kernel, 2. 6. 23, rc2; linux, kernel, 2. 6. 23, rc1; linux, kernel, 2. 6. 23; linux, kernel, 2. 6. 23. 10; linux, kernel, 2. 6. 23. 2; linux, kernel, 2. 6. 23. 1; linux, kernel, 2. 6. 23. 6; linux, kernel, 2. 6. 23. 5; linux, kernel, 2. 6. 23. 4; linux, kernel, 2. 6. 23. 3; linux, kernel, 2. 6. 23. 14; linux, kernel, 2. 6. 23. 7; linux, kernel, 2. 6. 22; linux, kernel, 2. 6. 22. 1; linux, kernel, 2. 6. 22. 5; linux, kernel, 2. 6. 22. 4; linux, kernel, 2. 6. 22. 7; linux, kernel, 2. 6. 22. 6; linux, kernel, 2. 6. 22. 16; linux, kernel, 2. 6. 22. 3; linux, kernel, 2. 6. 22. 22; linux, kernel, 2. 6. 22. 21; linux, kernel, 2. 6. 22. 20; linux, kernel, 2. 6. 22. 19; linux, kernel, 2. 6. 22. 2; linux, kernel, 2. 6. 22. 8; linux, kernel, 2. 6. 22. 9;
--	--

	linux, kernel, 2. 6. 22. 14; linux, kernel, 2. 6. 22. 15; linux, kernel, 2. 6. 22. 17; linux, kernel, 2. 6. 22. 18; linux, kernel, 2. 6. 22. 10; linux, kernel, 2. 6. 22. 11; linux, kernel, 2. 6. 22. 12; linux, kernel, 2. 6. 22. 13; linux, kernel, 2. 6. 21. 4; linux, kernel, 2. 6. 33; linux, kernel, 2. 6. 33. 2; linux, kernel, 2. 6. 33. 3; linux, kernel, 2. 6. 33. 4; linux, kernel, 2. 6. 33. 5; linux, kernel, 2. 6. 33. 6; linux, kernel, 2. 6. 32. 20; linux, kernel, 2. 6. 32. 19; linux, kernel, 2. 6. 32. 18; linux, kernel, 2. 6. 32. 17; linux, kernel, 2. 6. 32. 16; linux, kernel, 2. 6. 32. 15; linux, kernel, 2. 6. 32. 14; linux, kernel, 2. 6. 32. 13; linux, kernel, 2. 6. 32. 12; linux, kernel, 2. 6. 32. 11; linux, kernel, 2. 6. 31. 14; linux, kernel, 2. 6. 31. 13; linux, kernel, 2. 6. 33. 7; linux, kernel, 2. 6. 34; linux, kernel, 2. 6. 34. 1; linux, kernel, 2. 6. 34. 2; linux, kernel, 2. 6. 34. 3; linux, kernel, 2. 6. 34. 4;
--	---

		linux, kernel, 2. 6. 34. 5; linux, kernel, 2. 6. 34. 6; linux, kernel, 2. 6. 34. 7; linux, kernel, 2. 6. 35; linux, kernel, 2. 6. 35. 1; linux, kernel, 2. 6. 35. 2; linux, kernel, 2. 6. 35. 3; linux, kernel, 2. 6. 35. 4; linux, kernel, 2. 6. 36, rc1; linux, kernel, 2. 6. 36, rc2; linux, kernel, 2. 6. 36, rc3 以及更早的版本
2	Cisco IOS SSL VPN 拒绝服务漏洞	cisco, ios, 12. 4mr; cisco, ios, 12. 4; cisco, ios, 12. 4gc; cisco, ios, 12. 4mda; cisco, ios, 12. 4mra; cisco, ios, 12. 4sw; cisco, ios, 12. 4xa; cisco, ios, 12. 4xb; cisco, ios, 12. 4xc; cisco, ios, 12. 4xd; cisco, ios, 12. 4xe; cisco, ios, 12. 4xf; cisco, ios, 12. 4xg; cisco, ios, 12. 4xj; cisco, ios, 12. 4xk; cisco, ios, 12. 4xl; cisco, ios, 12. 4xm; cisco, ios, 12. 4xn; cisco, ios, 12. 4xp; cisco, ios, 12. 4xt; cisco, ios, 12. 4xv; cisco, ios, 12. 4xw;

		cisco, ios, 12.4xy; cisco, ios, 12.4xz; cisco, ios, 12.4ya; cisco, ios, 12.4yb; cisco, ios, 12.4yd; cisco, ios, 15.0m; cisco, ios, 15.0xa; cisco, ios, 15.1t; cisco, ios, 15.1%281%29xb1;
3	Cisco IOS 及 Unified Communication Manager 多个拒绝 服务漏洞	cisco, ios, 12.1; cisco, ios, 12.1t; cisco, ios, 12.1xi; cisco, ios, 12.1xj; cisco, ios, 12.1xl; cisco, ios, 12.1xm; cisco, ios, 12.1xp; cisco, ios, 12.1xq; cisco, ios, 12.1xr; cisco, ios, 12.1xs; cisco, ios, 12.1xt; cisco, ios, 12.1xu; cisco, ios, 12.1xv; cisco, ios, 12.1xy; cisco, ios, 12.1ya; cisco, ios, 12.1yb; cisco, ios, 12.1yc; cisco, ios, 12.1yd; cisco, ios, 12.1ye; cisco, ios, 12.1yf; cisco, ios, 12.1yh; cisco, ios, 12.1yi; cisco, ios, 12.2b; cisco, ios, 12.2bw;

	cisco, ios, 12. 2bx; cisco, ios, 12. 2by; cisco, ios, 12. 2cz; cisco, ios, 12. 2dd; cisco, ios, 12. 2dx; cisco, ios, 12. 2ex; cisco, ios, 12. 2ira; cisco, ios, 12. 2irb; cisco, ios, 12. 2irc; cisco, ios, 12. 2ird; cisco, ios, 12. 2ire; cisco, ios, 12. 2ixa; cisco, ios, 12. 2ixb; cisco, ios, 12. 2ixc; cisco, ios, 12. 2ixd; cisco, ios, 12. 2ixe; cisco, ios, 12. 2ixf; cisco, ios, 12. 2ixg; cisco, ios, 12. 2ixh; cisco, ios, 12. 2mra; cisco, ios, 12. 2mrb; cisco, ios, 12. 2sbc; cisco, ios, 12. 2sca; cisco, ios, 12. 2sch; cisco, ios, 12. 2scc; cisco, ios, 12. 2scd; cisco, ios, 12. 2sg; cisco, ios, 12. 2sra; cisco, ios, 12. 2srb; cisco, ios, 12. 2sre; cisco, ios, 12. 2su; cisco, ios, 12. 2sv; cisco, ios, 12. 2sxa;
--	---

	cisco, ios, 12.2sxb; cisco, ios, 12.2sxd; cisco, ios, 12.2sxe; cisco, ios, 12.2sxf; cisco, ios, 12.2sy; cisco, ios, 12.2sz; cisco, ios, 12.2t; cisco, ios, 12.2tpc; cisco, ios, 12.2xa; cisco, ios, 12.2xb; cisco, ios, 12.2xc; cisco, ios, 12.2xd; cisco, ios, 12.2xg; cisco, ios, 12.2xh; cisco, ios, 12.2xi; cisco, ios, 12.2xj; cisco, ios, 12.2xk; cisco, ios, 12.2xl; cisco, ios, 12.2xm; cisco, ios, 12.2xn; cisco, ios, 12.2xq; cisco, ios, 12.2xs; cisco, ios, 12.2xt; cisco, ios, 12.2xu; cisco, ios, 12.2xv; cisco, ios, 12.2xw; cisco, ios, 12.2ya; cisco, ios, 12.2yb; cisco, ios, 12.2yc; cisco, ios, 12.2yd; cisco, ios, 12.2ye; cisco, ios, 12.2yf; cisco, ios, 12.2yh;
--	--

	cisco, ios, 12. 2yj; cisco, ios, 12. 2yk; cisco, ios, 12. 2yl; cisco, ios, 12. 2ym; cisco, ios, 12. 2yn; cisco, ios, 12. 2yt; cisco, ios, 12. 2yu; cisco, ios, 12. 2yv; cisco, ios, 12. 2yw; cisco, ios, 12. 2yx; cisco, ios, 12. 2yy; cisco, ios, 12. 2yz; cisco, ios, 12. 2zc; cisco, ios, 12. 2zd; cisco, ios, 12. 2ze; cisco, ios, 12. 2zf; cisco, ios, 12. 2zh; cisco, ios, 12. 2zj; cisco, ios, 12. 2zl; cisco, ios, 12. 2zp; cisco, ios, 12. 2zu; cisco, ios, 12. 2zy; cisco, ios, 12. 2zya; cisco, ios, 12. 3; cisco, ios, 12. 3b; cisco, ios, 12. 3t; cisco, ios, 12. 3tpc; cisco, ios, 12. 3va; cisco, ios, 12. 3xa; cisco, ios, 12. 3xb; cisco, ios, 12. 3xc; cisco, ios, 12. 3xd; cisco, ios, 12. 3xe;
--	---

	cisco, ios, 12.3xf; cisco, ios, 12.3xg; cisco, ios, 12.3xi; cisco, ios, 12.3xj; cisco, ios, 12.3xk; cisco, ios, 12.3xl; cisco, ios, 12.3xq; cisco, ios, 12.3xr; cisco, ios, 12.3xs; cisco, ios, 12.3xu; cisco, ios, 12.3xw; cisco, ios, 12.3xx; cisco, ios, 12.3xy; cisco, ios, 12.3xz; cisco, ios, 12.3ya; cisco, ios, 12.3yd; cisco, ios, 12.3yf; cisco, ios, 12.3yg; cisco, ios, 12.3yh; cisco, ios, 12.3yi; cisco, ios, 12.3yj; cisco, ios, 12.3yk; cisco, ios, 12.3ym; cisco, ios, 12.3yq; cisco, ios, 12.3ys; cisco, ios, 12.3yt; cisco, ios, 12.3yu; cisco, ios, 12.3yx; cisco, ios, 12.3yz; cisco, ios, 12.3za; cisco, ios, 12.4; cisco, ios, 12.4gc; cisco, ios, 12.4md;
--	--

	cisco, ios, 12.4mda; cisco, ios, 12.4mr; cisco, ios, 12.4mra; cisco, ios, 12.4sw; cisco, ios, 12.4t; cisco, ios, 12.4xa; cisco, ios, 12.4xb; cisco, ios, 12.4xc; cisco, ios, 12.4xd; cisco, ios, 12.4xe; cisco, ios, 12.4xf; cisco, ios, 12.4xg; cisco, ios, 12.4xj; cisco, ios, 12.4xk; cisco, ios, 12.4xl; cisco, ios, 12.4xm; cisco, ios, 12.4xn; cisco, ios, 12.4xp; cisco, ios, 12.4xq; cisco, ios, 12.4xr; cisco, ios, 12.4xt; cisco, ios, 12.4xv; cisco, ios, 12.4xw; cisco, ios, 12.4xy; cisco, ios, 12.4xz; cisco, ios, 12.4ya; cisco, ios, 12.4yb; cisco, ios, 12.4yd; cisco, ios, 12.4ye; cisco, ios, 12.4yg; cisco, ios, 15.0m; cisco, ios, 15.0s; cisco, ios, 15.0xa;
--	---

	cisco, ios, 15. 1t; cisco, ios, 15. 1xb; cisco, ios_xe, 2. 5. 0; cisco, ios_xe, 2. 5. 1; cisco, ios_xe, 2. 6. 0; cisco, ios_xe, 2. 6. 1; cisco, unified_communications_manager, 6. 0; cisco, unified_communications_manager, 6. 1%281%29; cisco, unified_communications_manager, 6. 1%281a%29; cisco, unified_communications_manager, 6. 1%281b%29; cisco, unified_communications_manager, 6. 1%282%29; cisco, unified_communications_manager, 6. 1%282%29sul; cisco, unified_communications_manager, 6. 1%282%29sula; cisco, unified_communications_manager, 6. 1%283%29; cisco, unified_communications_manager, 6. 1%283a%29; cisco, unified_communications_manager, 6. 1%283b%29; cisco, unified_communications_manager, 6. 1%283b%29sul; cisco, unified_communications_manager, 6. 1%284%29; cisco, unified_communications_manager, 6. 1%284%29sul; cisco, unified_communications_manager, 6. 1%284a%29; cisco, unified_communications_manager, 6. 1%284a%29su2; cisco, unified_communications_manager, 6. 1%285%29; cisco, unified_communications_manager, 6. 0%281b%29; cisco, unified_communications_manager, 6. 0%281. 2114. 1%29; cisco, unified_communications_manager, 6. 0%281. 2121. 1%29; cisco, unified_communications_manager, 7. 0; cisco, unified_communications_manager, 7. 0%281%29; cisco, unified_communications_manager, 7. 0%281%29sul; cisco, unified_communications_manager, 7. 0%281%29sula; cisco, unified_communications_manager, 7. 0%282%29; cisco, unified_communications_manager, 7. 0%282a%29; cisco, unified_communications_manager, 7. 0%282a%29sul; cisco, unified_communications_manager, 7. 0%282a%29su2;
--	--

		cisco,unified_communications_manager,7.1%282a%29; cisco,unified_communications_manager,7.1%282a%29sul; cisco,unified_communications_manager,7.1%282b%29; cisco,unified_communications_manager,7.1%282b%29sul; cisco,unified_communications_manager,7.1%283%29; cisco,unified_communications_manager,7.1%283a%29; cisco,unified_communications_manager,7.1%283a%29sul; cisco,unified_communications_manager,7.1%283a%29sula; cisco,unified_communications_manager,7.1%283b%29; cisco,unified_communications_manager,7.1%283b%29sul; cisco,unified_communications_manager,7.1%283b%29su2; cisco,unified_communications_manager,8.0; cisco,unified_communications_manager,8.0%281%29;
4	Cisco IOS 多个网络地址转换漏洞	cisco,ios,12.1 cisco,ios,12.1t cisco,ios,12.1xi cisco,ios,12.1xj cisco,ios,12.1xl cisco,ios,12.1xm cisco,ios,12.1xp cisco,ios,12.1xq cisco,ios,12.1xr cisco,ios,12.1xs cisco,ios,12.1xt cisco,ios,12.1xu cisco,ios,12.1xv cisco,ios,12.1xy cisco,ios,12.1ya cisco,ios,12.1yb cisco,ios,12.1yc cisco,ios,12.1yd cisco,ios,12.1ye cisco,ios,12.1yf

	cisco, ios, 12. 1yh
	cisco, ios, 12. 1yi
	cisco, ios, 12. 2b
	cisco, ios, 12. 2bw
	cisco, ios, 12. 2bx
	cisco, ios, 12. 2by
	cisco, ios, 12. 2cz
	cisco, ios, 12. 2dd
	cisco, ios, 12. 2dx
	cisco, ios, 12. 2ex
	cisco, ios, 12. 2ira
	cisco, ios, 12. 2irb
	cisco, ios, 12. 2irc
	cisco, ios, 12. 2ird
	cisco, ios, 12. 2ire
	cisco, ios, 12. 2ixa
	cisco, ios, 12. 2ixb
	cisco, ios, 12. 2ixc
	cisco, ios, 12. 2ixd
	cisco, ios, 12. 2ixe
	cisco, ios, 12. 2ixf
	cisco, ios, 12. 2ixg
	cisco, ios, 12. 2ixh
	cisco, ios, 12. 2mra
	cisco, ios, 12. 2mrh
	cisco, ios, 12. 2sbc
	cisco, ios, 12. 2sca
	cisco, ios, 12. 2scb
	cisco, ios, 12. 2scc
	cisco, ios, 12. 2scd
	cisco, ios, 12. 2sg
	cisco, ios, 12. 2sra
	cisco, ios, 12. 2srb

	cisco, ios, 12.2sre
	cisco, ios, 12.2su
	cisco, ios, 12.2sv
	cisco, ios, 12.2sxa
	cisco, ios, 12.2sxb
	cisco, ios, 12.2sxd
	cisco, ios, 12.2sxe
	cisco, ios, 12.2sxf
	cisco, ios, 12.2sy
	cisco, ios, 12.2sz
	cisco, ios, 12.2t
	cisco, ios, 12.2tpc
	cisco, ios, 12.2xa
	cisco, ios, 12.2xb
	cisco, ios, 12.2xc
	cisco, ios, 12.2xd
	cisco, ios, 12.2xg
	cisco, ios, 12.2xh
	cisco, ios, 12.2xi
	cisco, ios, 12.2xj
	cisco, ios, 12.2xk
	cisco, ios, 12.2xl
	cisco, ios, 12.2xm
	cisco, ios, 12.2xn
	cisco, ios, 12.2xq
	cisco, ios, 12.2xs
	cisco, ios, 12.2xt
	cisco, ios, 12.2xu
	cisco, ios, 12.2xv
	cisco, ios, 12.2xw
	cisco, ios, 12.2ya
	cisco, ios, 12.2yb
	cisco, ios, 12.2yc

	cisco, ios, 12. 2yd
	cisco, ios, 12. 2ye
	cisco, ios, 12. 2yf
	cisco, ios, 12. 2yh
	cisco, ios, 12. 2yj
	cisco, ios, 12. 2yk
	cisco, ios, 12. 2yl
	cisco, ios, 12. 2ym
	cisco, ios, 12. 2yn
	cisco, ios, 12. 2yt
	cisco, ios, 12. 2yu
	cisco, ios, 12. 2yv
	cisco, ios, 12. 2yw
	cisco, ios, 12. 2yx
	cisco, ios, 12. 2yy
	cisco, ios, 12. 2yz
	cisco, ios, 12. 2zc
	cisco, ios, 12. 2zd
	cisco, ios, 12. 2ze
	cisco, ios, 12. 2zf
	cisco, ios, 12. 2zh
	cisco, ios, 12. 2zj
	cisco, ios, 12. 2zl
	cisco, ios, 12. 2zp
	cisco, ios, 12. 2zu
	cisco, ios, 12. 2zy
	cisco, ios, 12. 2zya
	cisco, ios, 12. 3
	cisco, ios, 12. 3b
	cisco, ios, 12. 3t
	cisco, ios, 12. 3tpc
	cisco, ios, 12. 3va
	cisco, ios, 12. 3xa

	cisco, ios, 12.3xb
	cisco, ios, 12.3xc
	cisco, ios, 12.3xd
	cisco, ios, 12.3xe
	cisco, ios, 12.3xf
	cisco, ios, 12.3xg
	cisco, ios, 12.3xi
	cisco, ios, 12.3xj
	cisco, ios, 12.3xk
	cisco, ios, 12.3xl
	cisco, ios, 12.3xq
	cisco, ios, 12.3xr
	cisco, ios, 12.3xs
	cisco, ios, 12.3xu
	cisco, ios, 12.3xw
	cisco, ios, 12.3xx
	cisco, ios, 12.3xy
	cisco, ios, 12.3xz
	cisco, ios, 12.3ya
	cisco, ios, 12.3yd
	cisco, ios, 12.3yf
	cisco, ios, 12.3yg
	cisco, ios, 12.3yh
	cisco, ios, 12.3yi
	cisco, ios, 12.3yj
	cisco, ios, 12.3yk
	cisco, ios, 12.3ym
	cisco, ios, 12.3yq
	cisco, ios, 12.3ys
	cisco, ios, 12.3yt
	cisco, ios, 12.3yu
	cisco, ios, 12.3yx
	cisco, ios, 12.3yz

	cisco, ios, 12.3za
	cisco, ios, 12.4
	cisco, ios, 12.4gc
	cisco, ios, 12.4md
	cisco, ios, 12.4mda
	cisco, ios, 12.4mr
	cisco, ios, 12.4mra
	cisco, ios, 12.4sw
	cisco, ios, 12.4t
	cisco, ios, 12.4xa
	cisco, ios, 12.4xb
	cisco, ios, 12.4xc
	cisco, ios, 12.4xd
	cisco, ios, 12.4xe
	cisco, ios, 12.4xf
	cisco, ios, 12.4xg
	cisco, ios, 12.4xj
	cisco, ios, 12.4xk
	cisco, ios, 12.4xl
	cisco, ios, 12.4xm
	cisco, ios, 12.4xn
	cisco, ios, 12.4xp
	cisco, ios, 12.4xq
	cisco, ios, 12.4xr
	cisco, ios, 12.4xt
	cisco, ios, 12.4xv
	cisco, ios, 12.4xw
	cisco, ios, 12.4xy
	cisco, ios, 12.4xz
	cisco, ios, 12.4ya
	cisco, ios, 12.4yb
	cisco, ios, 12.4yd
	cisco, ios, 12.4ye

		cisco, ios, 12.4yg cisco, ios, 15.0m cisco, ios, 15.0s cisco, ios, 15.0xa cisco, ios, 15.1t cisco, ios, 15.1xb cisco, ios_xe, 2.5.0 cisco, ios_xe, 2.5.1 cisco, ios_xe, 2.6.0 cisco, ios_xe, 2.6.1
5	Cisco IOS H.323 多个拒绝服务漏洞	cisco, ios, 12.1t cisco, ios, 12.1xi cisco, ios, 12.1xj cisco, ios, 12.1xl cisco, ios, 12.1xm cisco, ios, 12.1xp cisco, ios, 12.1xq cisco, ios, 12.1xr cisco, ios, 12.1xs cisco, ios, 12.1xt cisco, ios, 12.1xu cisco, ios, 12.1xv cisco, ios, 12.1xy cisco, ios, 12.1ya cisco, ios, 12.1yb cisco, ios, 12.1yc cisco, ios, 12.1yd cisco, ios, 12.1ye cisco, ios, 12.1yf cisco, ios, 12.1yh cisco, ios, 12.1yi cisco, ios, 12.2 cisco, ios, 12.2b

	cisco, ios, 12.2bw
	cisco, ios, 12.2bx
	cisco, ios, 12.2by
	cisco, ios, 12.2cz
	cisco, ios, 12.2dd
	cisco, ios, 12.2dx
	cisco, ios, 12.2ex
	cisco, ios, 12.2s
	cisco, ios, 12.2sb
	cisco, ios, 12.2sbc
	cisco, ios, 12.2sca
	cisco, ios, 12.2scb
	cisco, ios, 12.2scc
	cisco, ios, 12.2scd
	cisco, ios, 12.2sg
	cisco, ios, 12.2sra
	cisco, ios, 12.2srb
	cisco, ios, 12.2su
	cisco, ios, 12.2sv
	cisco, ios, 12.2sxa
	cisco, ios, 12.2sxb
	cisco, ios, 12.2sxd
	cisco, ios, 12.2sxe
	cisco, ios, 12.2%2818%29sxf7
	cisco, ios, 12.2%2818%29sxf8
	cisco, ios, 12.2sy
	cisco, ios, 12.2sz
	cisco, ios, 12.2t
	cisco, ios, 12.2tpc
	cisco, ios, 12.2xa
	cisco, ios, 12.2xb
	cisco, ios, 12.2xc
	cisco, ios, 12.2xd

	cisco, ios, 12. 2xg
	cisco, ios, 12. 2xh
	cisco, ios, 12. 2xi
	cisco, ios, 12. 2xj
	cisco, ios, 12. 2xk
	cisco, ios, 12. 2xl
	cisco, ios, 12. 2xm
	cisco, ios, 12. 2xn
	cisco, ios, 12. 2xq
	cisco, ios, 12. 2xs
	cisco, ios, 12. 2xt
	cisco, ios, 12. 2xu
	cisco, ios, 12. 2xv
	cisco, ios, 12. 2xw
	cisco, ios, 12. 2ya
	cisco, ios, 12. 2yb
	cisco, ios, 12. 2yc
	cisco, ios, 12. 2yd
	cisco, ios, 12. 2ye
	cisco, ios, 12. 2yf
	cisco, ios, 12. 2yh
	cisco, ios, 12. 2yj
	cisco, ios, 12. 2yk
	cisco, ios, 12. 2yl
	cisco, ios, 12. 2ym
	cisco, ios, 12. 2yn
	cisco, ios, 12. 2yo
	cisco, ios, 12. 2yt
	cisco, ios, 12. 2yu
	cisco, ios, 12. 2yv
	cisco, ios, 12. 2yw
	cisco, ios, 12. 2yx
	cisco, ios, 12. 2yy

	cisco, ios, 12. 2yz
	cisco, ios, 12. 2zc
	cisco, ios, 12. 2zd
	cisco, ios, 12. 2ze
	cisco, ios, 12. 2zf
	cisco, ios, 12. 2zh
	cisco, ios, 12. 2zj
	cisco, ios, 12. 2zl
	cisco, ios, 12. 2zp
	cisco, ios, 12. 2zu
	cisco, ios, 12. 2zy
	cisco, ios, 12. 2zya
	cisco, ios, 12. 3
	cisco, ios, 12. 3b
	cisco, ios, 12. 3t
	cisco, ios, 12. 3tpc
	cisco, ios, 12. 3va
	cisco, ios, 12. 3xa
	cisco, ios, 12. 3xb
	cisco, ios, 12. 3xc
	cisco, ios, 12. 3xd
	cisco, ios, 12. 3xe
	cisco, ios, 12. 3xf
	cisco, ios, 12. 3xg
	cisco, ios, 12. 3xi
	cisco, ios, 12. 3xj
	cisco, ios, 12. 3xk
	cisco, ios, 12. 3xl
	cisco, ios, 12. 3xq
	cisco, ios, 12. 3xr
	cisco, ios, 12. 3xs
	cisco, ios, 12. 3xu
	cisco, ios, 12. 3xw

	cisco, ios, 12.3xx
	cisco, ios, 12.3xy
	cisco, ios, 12.3xz
	cisco, ios, 12.3ya
	cisco, ios, 12.3yd
	cisco, ios, 12.3yf
	cisco, ios, 12.3yg
	cisco, ios, 12.3yh
	cisco, ios, 12.3yi
	cisco, ios, 12.3yj
	cisco, ios, 12.3yk
	cisco, ios, 12.3ym
	cisco, ios, 12.3yq
	cisco, ios, 12.3ys
	cisco, ios, 12.3yt
	cisco, ios, 12.3yu
	cisco, ios, 12.3yx
	cisco, ios, 12.3yz
	cisco, ios, 12.3za
	cisco, ios, 12.4
	cisco, ios, 12.4mr
	cisco, ios, 12.4sw
	cisco, ios, 12.4xa
	cisco, ios, 12.4xb
	cisco, ios, 12.4xc
	cisco, ios, 12.4xd
	cisco, ios, 12.4xf
	cisco, ios, 12.4xg
	cisco, ios, 12.4xj
	cisco, ios, 12.4xk
	cisco, ios, 12.4xl
	cisco, ios, 12.4xm
	cisco, ios, 12.4xn

	cisco, ios, 12.4xp
	cisco, ios, 12.4xt
	cisco, ios, 12.4xv
	cisco, ios, 12.4xw
	cisco, ios, 12.4xy
	cisco, ios, 12.4xz
	cisco, ios, 12.4ya
	cisco, ios, 12.4yb
	cisco, ios, 12.4yd
	cisco, ios, 12.4ye
	cisco, ios, 15.0m
	cisco, ios, 15.0xa
	cisco, ios, 15.1t
	cisco, ios, 15.1xb
	cisco, ios_xe, 2.5.0
	cisco, ios_xe, 2.5.1
	cisco, ios_xe, 2.6.0

产业动态

国家测绘局：2015年可全国虚拟旅游

来源：南方都市报

下一步，将实现市县联网，加快数字省区建设和国家数字平台的建设。到2015年，实现国家、省市全社会数字平台全线贯通，全社会能够享受到数字化城市的便捷服务，在网上，就能玩遍全国各地的旅游景区。

——国家测绘局国土测绘司一负责人

在电脑上用鼠标点开“临沂地理信息公众服务系统”，除了可以看到城市的各条道路、建筑物的虚拟立体图外，还可以进行“虚拟旅游”，通过鼠标和键盘就可以进入三维的游博物馆内看精美的展品等。近日，推动城市数字化建设的临沂市测绘与地理信息局成立，这是我国第一个地级市测绘与地理信息局。这意味着，我国的神秘而难懂的测绘数据不再局限于为政府部门服务，其服务范围扩展到广大群众的衣食住行等领域。

国家测绘局国土测绘司一位不愿意透露姓名的负责人告诉南都记者，到2015年，地理信息将实现国家、省、城市全线贯通，大家可以在网上去全国各地“虚拟旅游”。

现行测绘管理体制混乱

新成立的临沂市测绘与地理信息局是我国首个地级市的测绘与地理信息局，属于临沂市国土资源局的二级局，为副处级，整合了临沂国土局测绘科、测绘院等部门。

国家测绘局一位不愿透露姓名的负责人告诉南都记者，目前，我国测绘系统管理体制不顺畅，五花八门。在国家层面，国家测绘局是国土资源部的二级局；而在地方则比较混乱，有的地方测绘部门属于国土部门管辖，有的则属于规划部门管辖，有的测绘部门和国土部门是一个并列的两个部门，有的县级测绘局还没有挂牌。

“为了管理方便，我们希望地方各级政府能够保持国家的管理体制，统一名称，但这需当地编制部门的批准。”国家测绘局负责人告诉南都，除临沂测绘与地理信息局外，我国第一个省级测绘与地理信息局——8月底成立的浙江省测绘与地理信息局也是向国家的管理模式“看齐”：属国土部门管辖。

临沂市之所以能成为我国第一个市级测绘与地理信息局，从2006年开始，国家测绘局启动“数字区域地理空间框架建设示范”基础测绘项目，在全国28个省份选出2-3个城市开展数字城市建设，包括临沂在内的78个城市(区)作为数字城市建设试点。

截止到目前，山西太原、湖北潜江、浙江嘉兴、黑龙江齐齐哈尔、山东临沂5个城市的“数字区域地理空间框架建设示范”基础测绘项目已经获得国家验收。临沂率先成立了测绘与地理信息局。

国家测绘局的负责人介绍，其他4个获得验收的城市有望年底成立市级测绘与地理信息局。

国土资源部副部长、国家测绘局局长徐德明表示，全国第一个市级测绘与地理信息局挂牌成立，是测绘管理模式和方式的重大变革，对加快数字城市建设、监测国情以及地理信息产业发展，具有推动作用。

测绘数据服务对象拓宽了

在过去，测绘局被人看着是生产地理信息数据的地方，因为过去原来地理信息存在涉密问题，测绘数据只是授权政府部门、科研机构使用，也不对外出售，测绘部门生产出来的大量数据通常处于闲置、封闭状态。对普通群众来说，测绘数据是一个复杂而神秘的东西，是乎离人们生活很遥远。

临沂新成立的测绘与地理信息局就有监管数字城市建设，管理很运用地理信息的职能。将测绘数据分为三个版本来服务不同的人群：基础标准版只是供政府等相关内网使用，是涉密版本；政务版主要是涉及执法、规划、城市管理、救援指挥调度等，如将城市的每个路灯都进行了编号，报修时只需报编号就可以马上派人去抢修，调度速度大大加快。

公众版是过滤了涉密信息外，其服务数据最多、最全。“数字临沂地图网”就是面向公众，细到某一条公路，某一家宾馆有多少床位等等，还可通过三维画面去某个景点虚拟旅游，可以看到与现实一样各种展品的实景图等。

临沂国土资源局测绘管理科科长胡传合介绍，数字平台面对政府和公众版都是无偿的，只是在为公众服务数字平台中，一些地图标注的功能是有偿使用的，如标注企业名称、宣传定位等，还包括在信息平台中做的广告等。

国家测绘局的负责人表示，建设数字城市是一项惠民的举措，在国家层面也鼓励对数据平台上进行个人和企业的增值服务，将会产生强大的经济效益。

调整经济结构转型

国家测绘局副局长宋超智表示，希望临沂市测绘与地理信息局围绕着临沂市转变经济发展方式，调整经济结构，推动经济社会发展。

国家测绘局负责人解释说，测绘与地理信息产业，是要把地图平台、网络和 windows 操作平台结合起来，实现全社会信息的对等。大家能在很短的时间内了解到该地区的人口分布、资源分布、产业结构、人才资源以及政府发展和产业规划。上下游相邻的国家、地区就能以此互为前提、互为依托，进行分工协作，形成一个产业集群。轻松实现招商引资和产业结构调整。外出招商引资也比传统招商方式更加简便捷。

2015年实现全国数字平台通联

国家测绘局国土测绘司不愿透露姓名的负责人告诉南都记者，对于新成立的测绘与地理信息局，要求服务是全方位的。同时，在以后数字试点城市，要加强对手机查询、移动查询等新的查询方式的技术加以研发，满足各种人群的服务需要。

该负责人还透露，下一步，将实现市县联网，加快数字省区建设，和国家数字平台的建设。到

2015 年，实现国家、省市全社会数字平台全线贯通，全社会能够享受到数字化城市的便捷服务，在网上，就能玩遍全国各地的旅游景区。

谷歌街景服务在德国遇到强烈抵制 上万人退出

来源：赛迪网

9 月 20 日消息，据本周一出版的德国《明镜》周刊报道称，谷歌街景导航服务在德国遇到的抵制比它原来预料的强烈的多。成千上万人选择退出这项服务。

在 10 月 15 日最后期限之前，数十万德国人已经通知谷歌说，他们不想让自己的家或者企业出现在谷歌街景服务中。谷歌街景有在街道级拍摄的全景静态照片。

据接近谷歌的知情人士说，谷歌在 8 月份曾表示它预计有数十万德国当地居民和企业主要求谷歌在发布图像的时候对对楼房做模糊化处理。

消费者事务部曾预计有 20 多万个地址会提出这种申请。

谷歌上个月发布了一些计划，要在今年晚些时候在德国的 20 多个城市推出街景服务。谷歌街景服务目前已经在全球 20 多个国家推出。但是，谷歌宣布的这个消息引起了德国人对安全和隐私的担心。

德国汉堡的数据保护官员 Johannes Caspar 说，他认为谷歌将尊重德国公民的愿望。但是，他说，他怀疑谷歌是否能够正确地处理这样多的申请。

鉴于对街景服务的争议，德国政府正在考虑对在线数据保护制定新的法律。德国内政部长德梅齐埃(Thomas de Maizière)本周一将在柏林主持召开有关这个问题的高级会议。

惠普完成对 Fortify Software 并购

来源：新浪科技

北京时间 9 月 22 日晚间消息，据国外媒体报道，惠普周三宣布，已完成对互联网安全软件厂商 Fortify Software 的并购。

Fortify Software 在数据应用安全分析领域占有领先地位，其技术可以防范恶意软件攻击，从而帮助企业降低商业风险。

通过 Fortify Software 的技术和产品，惠普将为用户提供一流的安全解决方案，保证用户从开发到运营整个环节的安全。

惠普上个月宣布收购 Fortify Software，但并未透露具体的交易金额。

Facebook 称数据库软件问题导致严重故障

来源：腾讯科技

北京时间 9 月 25 日消息，据国外媒体报道，Facebook 软件工程主管罗伯特·约翰森（Robert Johnson）表示，Facebook 周四出现的故障是由于数据库软件问题而导致的。

约翰森在博客中表示，此次故障是由于软件问题引起的，这款软件旨在检测和修复缓存中的错误。他写道：“导致此次故障的关键原因在于针对错误环境的一次不当操作。一款旨在检测缓存中无效配置值的自动化系统软件导致了此次故障。”

约翰森介绍说，这款自动化软件原本旨在修复缓存中无效的配置值，但由于未能正常工作，导致周四 Facebook 网站出现大范围故障。

周四的故障一共持续了两个半小时，约翰森表示：“这是过去四年来 Facebook 所经历的最严重的故障。”约翰森并未表示 Facebook 是否会为广告客户提供补偿。

目前，Facebook 已经从创始人马克·扎克伯格（Mark Zuckerberg）的一个大学实验室项目发展成为全球最受欢迎的社交网站，并且在某些方面与谷歌和微软展开竞争。因此，用户和广告客户对于 Facebook 的故障也越来越挑剔。

约翰森在博客中也提到了这一点。约翰森写道：“我们再次就此次故障表示道歉，同时我们希望用户知道，我们非常重视 Facebook 的运行与可靠性。”

新版阿里旺旺可识别木马 将于一个月里面世

来源：荆楚网-楚天都市报

往支付宝里打款，遭遇黑客侵袭，网购资金被劫至骗子的账户。连日来，本报推出的“网购黑客陷阱调查”引起了多方关注。昨日，阿里巴巴集团高层对本报报道进行回应。

阿里巴巴集团资深副总裁、大淘宝首席品牌官王帅表示，感谢本报揭此骗局，并表示淘宝网会配合公安机关坚决打击网络灰色产业链。

淘宝：新阿里旺旺 1月内上线

淘宝网信息安全部总监倪良称，今年5月份，淘宝网首次检测到了“劫持木马”，这是一种新型的网络诈骗手段。从淘宝客服接到的投诉来看，8月份这种劫持木马开始猖獗。

淘宝网此前已采取了几大措施：包括强化用户安全宣传工作，让用户认清了该骗术的本质并提供解决方案；联合各大杀毒厂商拦截此类木马，并实时将该木马的最新标本发给杀毒厂商予以查杀；加强了传输文件的内容检测，对于存在风险的文件禁止传输。不过，从本报记者的调查以及读者反馈看，通过阿里旺旺传播的木马病毒仍有“漏网之鱼”。

淘宝网信息安全部经理隋东平、淘宝网公众与客户沟通部资深经理赵景鹏17日专程从杭州赶往本报编辑部沟通。隋东平表示，将改进聊天工具阿里旺旺的功能，加强安全防范。在新的阿里旺旺中，将设置自动解包功能，即对于卖家发过来的压缩文件能够自动解开，对于其中存在风险的文件，阿里旺旺自动过滤掉。此外，还将在顾客网购时告知最近常见的诈骗手段，避免更多人上当受骗。

对于此前有淘宝客服人员称，“消费者资金被劫皆因操作不当造成”，淘宝网相关负责人承认，此言欠妥。淘宝网有义务保证卖家和买家之间的顺畅的、无障碍的交流。传输文件也属于买卖双方正常交流的一种方式。

据悉，能识别木马病毒的购物聊天工具阿里旺旺将于1个月里面世。

支付宝：与银行开展风险联防

支付宝副总裁井贤栋也对本报报道进行了回应。

他称，目前以钓鱼网站、黑客侵袭为特征的网络诈骗产业链初步形成，成为威胁网购者利益的第一杀手。深藏在背后的这股势力利用网民对网络犯罪的警惕性不高，通过高科技手段进行违法犯罪，给网民造成了巨大的损失，阻碍了包括支付宝在内的整个中国电子商务产业的发展。

井贤栋说：“作为国内著名的电子支付平台，支付宝用户及公司深受其害。我们对于受害用户的遭遇深表同情，并对此类违法犯罪行为深感愤慨，我们认为这不但是对用户及支付宝公司的侵害，更是对整个中国互联网产业发起的挑战。”

据称，支付宝公司与各大银行推进相关合作，开展风险联防计划，并与互联网合作伙伴建立更为强大的绿色安全支付圈，为用户打造一个安全、便捷的网络支付环境。

被骗的钱该谁负责

对于阿里巴巴高层的回应，部分受骗网友并不满意。

山东青州受骗者李云鹏认为，淘宝和支付宝应该赔偿损失。而在上述高层回应中，对赔偿只字未提，显然是避重就轻。

上海受骗者李淼说，淘宝网称此前已经采取了措施，但这些措施根本没有起到应有的效果。

广东珠海受骗者卢灵玲一直负责受骗人数和金额的统计，从 9 月 13 日本报首次报道“网购黑客陷阱调查”至今，有统计的受害人数又增加了 25 人，受骗金额增至 15.1 万。她认为，淘宝、支付宝在明知存在安全漏洞的情况下仍然没有采取有效的应急措施，导致受骗者继续增多，应承担直接责任。

目前，相关方面并未将被骗金额进行追讨。有网友表示，在这一步完成之后，将对涉事单位提起民事诉讼。 记者夏宇

几种常见网购骗术

除了木马侵袭、钓鱼网站外，阿里巴巴集团还公布 3 种常见的骗术及防骗技巧。

1、虚假的客服电话欺诈

在网上搜索“淘宝网客服电话”，你会发现一堆的虚假客服电话。当打通这个电话后，对方会利用各种理由诱导您进行汇款，从而导致被骗。消费者务必到官方网站去查找客服电话。

2、超低价诱导线下汇款

当搜索到一款商品价格超低时，卖家可能谎称商品是“漏税”或“盗窃”得来的，不支持支付宝交易，要求买主通过银行汇款方式支付货款，导致买家受骗。消费者须严格按支付宝流程进行网购操作。

3、用退款骗取买家钱款

当成功购买商品后，有卖家可能会告诉买家这件商品还可以有折扣，要求买家申请退款，并且嘱咐要选择“已经收到货——卖家应退还我的钱：X 元”的选项。

对此请不要因为卖家的折扣，在“没有收到货”的情况下，选择已经收到货，否则易导致货财两空。

谷歌微软和 IBM 竞标美国联邦总务局云计算合同

来源：腾讯科技

北京时间 9 月 23 日消息，据国外媒体报道，面对美国联邦总务局的云计算合同招标，谷歌、微软和 IBM 展开了激烈的角逐。

早在 7 月 30 日，美国联邦总务局邀请软件生产商谷歌、微软和 IBM 竞标联邦机构电子邮件和协作应用程序供应商，并要求它们提交各自的标书。美国联邦总务局规定的投标有效期限为 9 月 30 日。

美国联邦总务局负责美国政府采购和管理美国联邦资产，它目前采用的 IBM 服务平台 Lotus Notes，整合了电子邮件和文件应用程序，提供给美国联邦总务局的 15000 名雇员使用。这些应用程序安装在美国联邦总务局的服务器及其用户的电脑上。

由于联邦政府计划升级其技术基础设施，美国联邦总务局决定升级换代，采用最近流行的云计算模式。这意味着美国联邦总务局需要采购谷歌、微软和 IBM 等软件生产商通过网络提供的远程数据中心的程序。一般来说，享有这三家软件生产商提供的云计算电子邮件服务的公司，只要支付每位用户每月 3 美元到 5 美元的基本价格，就可以通过网络浏览器使用这些应用程序。

谷歌、微软和 IBM 目前均已提交了标书，美国联邦总务局通讯和营销副主管 Sahar Wali 确认说。然而，这三家公司拒绝透露有关他们已提交的标书的具体内容。因为没有公司想在投标阶段就因为过多谈论其标书内容而丧失自己的竞争优势。

IBM 只声称其提交了基于网络的 LotusLive iNotes 软件供美国联邦总务局参考。微软则声称提交了一套基于云计算的讯息传递与协作解决方案 Business Productivity Online Suite，并确认其标书中包含有电子邮件和其他协作应用程序，但是拒绝透露更多细节。谷歌提交了其政府版企业应用套件 Google Apps，该套件包含有电子邮件、文件、电子表格和幻灯片等应用程序。

安全市场面临重新洗牌

来源：ZDNET

英特尔收购 McAfee 已经过去一个多月，但直到今天为止，关于这一收购案的喧嚣仍然未止，关于这一收购案的揣测仍在继续。McAfee 官方曾多次发表声明，披露了对这次收购案长远效益利好的见解，McAfee 首席执行官兼总裁 Dave DeWalt 两次在其官方博客撰文。与业界近乎沸点的关注度相比，英特尔官方对此收购事件的态度异常平静，除了在事件初期，解释了云计算、嵌入式安全等纯技术角度的考虑之外，并没有对资本运作、产业影响予以置评。似乎将 McAfee 收入麾下，只是其战略布局中的其中一步而已，而在此时将自身的整体构想公之于众而略显草率？抑或是以英特尔长久以来在 IT 业界的创新领袖地位，使得业界过高的给予了这次事件的评估等级？

但随之而来的惠普收购 ArcSight 刚好迎合了之前的故事，将笔者上文“抑或是”的揣测完全推翻。在安全市场的收购喧嚣暂时归于平静的时候，不妨让我们一起探究安全受宠背后的源动力，英特尔收购 McAfee 明显给技术创新已显颓势的安全市场注入了新的活力，将安全的重要性提升到了新的高度，也使得安全市场在不远的将来面临重新洗牌。

洗牌之：创新性安全公司渐成香饽饽

在英特尔收购 McAfee，相关评估机构，业界对这起收购的质疑不断。为什么那么多的安全创新公司，会选择 McAfee，而且估价过高。笔者认为这样的质疑，似乎没有什么必要。简单来说，英特尔视创新为己任，选择一家有过硬创新技术的公司理所当然。而 McAfee 有这个资本，笔者曾在“五大印象：英特尔的 McAfee”一文中已经提过，这里不再累述。全安全产品线、强大的研发体系和现有 GTI 架构，最大的独立安全厂商，都足以让 McAfee 值 76.8 亿美金。而笔者认为，真正撬开英特尔口袋是 McAfee 在安全市场的战略愿景。在年初 McAfee 连续两笔收购，买进 2 家移动安全厂商，而这正与英特尔的多元化战略部署，看重移动互联网市场美丽蓝图的构思不谋而合，显然不仅仅是 McAfee 这样的传统安全巨头受到青睐，创新性安全公司的前景将更为乐观。所以对于在移动互联网、WEB 应用创新方面有着良好发展势头的创新性安全企业，将会逐渐成为香饽饽，英特尔和惠普为他们打开了一扇门，门的后面更加光明，安全市场也将更加光明。近日，笔者又一次遇到了 RSA 公司总裁亚瑟.W.科维 络，并与他交流了关于创新性安全公司的话题，他依然坚持 3 年前的观点，“独立安全厂商已难独立生存，创新性安全公司将更多的被收购。”

洗牌之：安全联姻基础架构早有预兆 将走进基础架构核心

其实在更早的时候，安全联姻基础架构就早有预兆。EMC 收购传统安全厂商 RSA，华为联姻赛门铁克，把时间轴拉的更远些，IBM 收购 ISS，Juniper 收购 Netscreen，赛门铁克收购 Veritas 等等。安全与安全，基础架构与安全，安全与基础架构之间的收并购从未停止过。而基础架构与安全的联姻在近几年却略显平淡，直到英特尔收购 McAfee，并且将安全未来所能发挥的作用更加深入，不仅仅再局限于平台化的安全支撑，将真正走进芯片，走进基础架构的核心。

洗牌之：安全融入网络 更容易走进云计算

云计算的大潮任谁都无法忽视，虽然关于云计算的应用案例少的让我们以为其是幻象，不论是“爱之深、恨之切”，“云计算革命尚未成功，同志还需努力”，“蹒跚学步阶段”，让我们有理由相信云计算的真正到来将是真正理性的云计算，将是真正服务于企业应用的云计算。而业界也正为之不懈努力。收购也罢，技术创新也好，在云计算的巨大分水岭前，IT 巨头们风风火火抢占云计算解决方案的制高点，而作为支撑企业未来应用的关键要素之一，安全与虚拟化、数据存储同样重要，而且未来的安全、存储一定会网络化，而且基于服务器的应用，所以传统的电信厂商和 IT 厂商谁将更早的掌控了安全，掌控了其他要素，就更容易走进云计算。

洗牌之：基于软件的安全将如何走下去

杀毒软件无用论，免费的话题，近几年的论调此起彼伏。在 2008 年 RSA 大会上，钱伯斯曾直

接提出“杀毒软件无用论的”观点，而关于杀毒软件免费的话题，在国内外喧嚣。不仅让我们担忧的是，基于软件的安全在未来将如何走下去，是消失在安全市场的变革中，还是通过免费寻找其他的增值业务模式，还是凝结成更紧密的战略联盟，通过共享相关资源，为用户和企业更好的服务，还是坚持技术上的创新，在企业应用端，用户桌面取得更大的成长空间，还是通过开拓新兴的应用安全软件，来博取更广阔的生存环境。不妨让我们拭目以待，共同思考。

洗牌之：安全促进平台化的融合统一

就目前来看，收购安全公司的意图，主要还是促进基础架构平台化的进一步融合统一。从惠普连续的两笔安全软件收购来看：惠普收购 Fortify，看重以发现软件代码中可能存在的安全漏洞和法规遵从问题。收购 ArcSight，看重其企业内控和规范监控。

这些都能帮助惠普迅速完成基础架构、融合架构的支撑。所以要实现平台化的融合统一，安全尤其重要，因为未来从虚拟化、应用开发、管理到企业内控，安全的短板都已经成为制约他们全面完成基础架构平台化的瓶颈之一。

华为将史无前例地向客户开放其计算机源代码

来源：网易科技

据《金融时报》报道，华为管理人士透露，华为将史无前例地向客户开放其计算机源代码，并在进行合同竞争时允许外部公司检查其网络设备产品。报道称，华为正在提高透明度，希望打消外界对公司在美国引发的国家安全问题担忧。分析称，华为此举将影响整个行业，因为设备销售商在提供安全检查方面与监管机构的分歧越来越大。

今年早些时候，华为同意印度政府的要求，向其提供一组关键的软件代码，但此举遭到希望竞争对手的批评。不过华为这一行为帮助推翻了印度对中国设备进口的禁令。

华为目前正在竞争美国第三大运营商 Sprint Nextel 的一个合同，帮助其扩张无线宽带网络。

但是由于美国政客反对该交易，华为出台一个三管齐下的安全计划，希望藉此打消美国方面的顾虑。除了在特定条件下提供源代码外，华为还将向信息安全专家提交其产品进行检查，以确定这些产品并不包含可用于间谍或使得网络容易遭受攻击的技术。客户也可以选择是否由华为的工程师、雇员或者信赖的第三方对其网络进行服务或提供软件升级。

一位华为高管表示，这些承诺的目的是为该公司打造“世界领先的透明程序”。

华为目前聘请一家名为 Amerilink 的顾问机构为其提供咨询意见，该机构的创始人和董事长威廉·欧文斯（William Owens）曾担任克林顿总统时期美军参谋长联席会议副主席，董事会成员包括曾任众议院多数党领袖的理查德·普哈特（Richard Gephardt）和世界银行前行长沃尔芬森（James Wolfensohn）。

微软敦促电子隐私法案 以助云计算等新技术的发展

文章来源：中国计算机安全

9 月 24 日消息，据国外媒体报道，微软公司正在敦促美国立法机构检查电子隐私法案，以帮助诸如云计算这样的新技术的发展。未来五年，云计算的预计销售将翻番。

微软公司法律顾问 Brad Smith 昨日在华盛顿举行的一个参议员司法委员会听证会上说，越来越多的数据储存在远程服务器而不是个人电脑里。1986 年的电子法案需要更新，以便帮助消费者就其信息安全建立信心。

“法律需要与时俱进，” Smith 在听证会结束后说。云计算将是“未来的一个重要部分，也是我们显著所做的一个重点”。

根据 Gartner 的数据，在远程计算机服务器上收集和储存数据被称为云计算，其全球销售额将在 2014 年末从去年的 586 亿美元上升至 1488 亿美元。Smith 说，如果消费者担心在线安全的话，这将限制行业发展。

来自谷歌、亚马逊、软件公司 Salesforce 和 Rackspace Hosting 公司的代表今天将出席听证会。

微软公司销售诸如 HealthVault 的云计算软件，可以帮助病人通过在线存储数据控制管理慢性疾病。微软公司还销售 Windows Azure 软件，可以让诸如 Domino's Pizza 这样的公司管理订单。

电子通信隐私法 1986 年由美国国会通过，目的是保护个人隐私信息的安全。

“我们意识到企业和个人消费者只会使用那些他们认为信息被很好保护的新技术，” Smith 说。

法案提供了保护电子信息的不同级别。近 180 天的电子邮件比旧邮件更安全。存在个人电脑硬盘上的信息比存在“云端”的更安全。

“微软支持在将数据从个人电脑转移到云端时不损害消费者隐私权的变化，” Smith 说。

参议员 Patrick Leahy 称委员会将开始着手调查修改法律的工作，但是没有给出具体时间表。

技术前沿

《科学》：多国科学家首次实现双光子的量子游走

来源：新华网

英国布里斯托尔大学等机构的研究人员在新一期美国《科学》杂志上报告了量子计算机研究领域的新进展。领导研究的杰里米·奥布赖恩教授认为，这一进展可能使量子计算机面世的时间提前到 10 年之内。

奥布赖恩教授领导的这个小组由英国、日本、以色列和荷兰等多国研究人员组成。他们成功研发出一种可用于量子计算的硅芯片，让两个完全相同的光子通过刻录在硅芯片上的光学网络，实现了名为“量子游走”的物理过程。过去，人们只实现过单光子的量子游走，而本次研究首次实现了双光子的量子游走。

奥布赖恩教授说，从单光子到双光子是一个巨大的跨越，每添加一个光子，量子计算机可解决问题的复杂程度是成指数增加的，比方说单光子的量子游走可以带来 10 个结果，那么双光子的量子游走将可以带来 100 种结果。

他说：“许多人认为量子计算机至少要再等 25 年才会出现，但我们相信，在使用这种新技术之后，10 年内就可能出现超越传统计算机的量子计算机。”

量子计算机是建立在量子力学规律基础上的计算机，它与传统计算机的一个主要区别是，传统计算机只使用 1 和 0 两种状态来记录数据和进行计算，而量子计算机可以同时使用多个不同的量子态，因此具有更大的信息存储和处理能力，被认为是未来计算机发展的方向。

数据中心制冷技术面临的新挑战

来源：机房 360

在几乎所有的 IT 部门都采取各种各样的措施向云计算开始靠拢的时候，数据中心的冷却技术将面临更多的挑战。在云计算的环境下，数据中心将向虚拟化，高密度化方向发展，面临更广泛和更频繁的负载。这与传统的静态数据中心相比，对冷却技术提出了一系列的挑战。

制冷专家认为，在这样的环境下，数据中心的冷却系统需要有迅速调整的能力。一个高度自动化，可以快速调整制冷效率的冷却系统才能更好的使用这样的环境。

数据中心密度的提高

在旧的数据中心，服务器的排列永远都是一成不变的，数据中心内的服务器密度也是这样，所

以对冷却系统的要求也是如此，不过刀片式服务器的出现改变了这一局面。在计算量需求日益增大的数据中心内，随着刀片式服务器的应用，服务器密度的越来越大，因而创造的热量也越来越多，因而对冷却系统的要求也越来越高。而虚拟化的应用也是冷却系统面临的额外挑战，这一技术进一步提高了数据中心内服务器的负荷密度。

在云环境下的数据中心，每个机架的功率已经达到了 10 千瓦左右。而密度的提高只是问题的一部分。冷却系统面临的最大的挑战是数据中心内负载的变化引起的热量处理的变化。在云计算环境下的高密度数据中心内，几乎每个时间段内，每个区域内服务器的负载都不一样，他们产生的热量也都不一样。如果一直对服务器使用同一种冷却方案显然不能够保证数据中心的高效工作。

解决该问题的方案之一是采取冷通道/热通道遏制技术。这种技术将冷空气与热空气隔绝开来，在空气与冷空气混合之前将热空气排出，从而提高制冷的效率。

但是，很明显，这种冷却技术虽然解决了数据中心内密度过高的问题，但仍然不能做到精确的制冷。在一个数据中心内部，服务器的负载并不是平均的，而且会随着时间的推移而发生变化，托管服务提供商和运营商很清楚这一点，他们已经学会了如何处理这一点。例如，在机架下方安装不同密度的穿孔瓷砖，并可以根据程序调节冷空气的送风量。根据不同的需求来提供不同的冷却能力，最大效率的利用冷却系统。一个智能化的冷却系统显然更加能够面对高密度数据中心的挑战。

新型的空调系统

在云计算的环境下，需要一个能够作出快速反应的空调系统。

在传统的空调系统中，改变制冷量需要手工的操作。而手工操作的速度并不能保证及时赶上环境的变化。工程师们选择不同的方法来增强空调系统的活力。与传统静态的空调系统相比，一个可以自动调节的空调系统会更加有效率。

例如，在空调系统中加入一种可以调节空气量的装置。可以通过监测周围环境的变化而调整整个系统的空气流量，从而改变整个空调系统的制冷效果。这些监测环境的传感器分布在机架的周围以及顶部。可以提供实时的温度变化状况。

此外，一种将蒸发式冷却和干燥剂结合在一起的空调系统虽然不具有自动调节的能力，却可以大幅提高冷却的效率，并至少降低一半以上的能源消耗。该空调系统是由 NREL（美国国家资源再生资源实验室）压法的。这种名为 DEvap 的空调是干燥剂增强蒸发式空调的代表，这是一种使用膜技术，将蒸发式空调的冷却效率和液体除湿盐的干燥潜力合并在一起的新型冷却概念。据 NREL 称，该空调的在制冷过程中将比现在最顶级的空调少使用 50%到 90%的能量。

服务器的负载变化

虽然对于机架等设备来说，通常会有快速自动冷却的解决方案。但是，在服务器负载较大的时候，还是会由于冷却系统提供不了足够的冷却能力而容易产生一些问题，甚至是一些严重的后果。

传统的冷却系统会根据负载做出一些实时响应，但这仅局限于负载的变化不大的时候。而当服务器的负载出现较大的变化时，就会出现上面的情况了。

在今天的自动化冷却系统中，虽然可以处理上述的问题，但也带来了一些新问题。在测试中，自动化冷却系统也不能频繁的处理服务器的负载变化。可以想象，如果突然将数据中心的冷却能力在一个小时由 500 吨下降到 100 吨，那么冷却机组只能关闭自己来防止过冷导致冻结它的阀门。

至少，如果没有自动化的系统，倒不会出现上述的情况。冷却机组不会自动关闭，因为那样的话，如果遇到了一些突发的情况，所有的冷却机组都会自动关闭，将没有冷却机组会继续工作。一旦冷却机组关闭了，它至少需要 20 分钟才能恢复工作。

显然，进一步的提高冷却效率才能彻底解决这一问题。通过遏制技术或者其他技术尽量减少服务器负载变化产生的影响才能给冷却机组减轻压力，给冷却系统充分的响应时间。

在云计算环境下的数据中心内，冷却系统面临的挑战不只有适应高密度发展的需求，如何提高自身的能源使用效率，发展低碳，绿色的技术也成为了当前的目标之一。这就需要多方面的合作，为建设更加高效，更加绿色的数据中心共同做出努力。

黑客攻防

Dos 采用 web 服务器攻击

来源：ZDNET

近日，安全研究人员发现了一个新的僵尸网络，一个使用 Web 服务器，而不是通常黑客们使用的个人电脑来发动的拒绝服务(DoS)攻击。

攻击者只要访问这台服务器，并简单的填写需要攻击目标的 IP 地址、攻击持续时间、端口即可。页面下方还写着“不用对你们的朋友使用它。”

安全公司 Imperva 在周三表示，他们检测了很多网络状况十分糟糕的企业以及分析了攻击 Google 的代码，之后，他们发现了一个包含有 300 台 Web 服务器的僵尸网络。Imperva 首席技术官 Amchai Shulman 表示，十多年前，Web 服务器被用于类似的攻击上，但后来其已经被大量的 Windows 平台个人电脑所取代。

Imperva 发现的 DoS 攻击中，两个 Web 服务器都来自一个总部设在荷兰的未知主机供应商。Shulman 表示，该供应商已经意识到了这个问题。

他还表示，看起来，这些 Web 服务器使用了一些开发中包含有脆弱代码的 PHP(一种用于处理网页的计算机语言)，这里面包含有大量漏洞，这些漏洞影响了服务器上运行的 Apache、Microsoft Internet Information Services (IIS)，或者其他服务器应用程序。

Shulman 展示的一个截图显示，攻击者设计了一个非常简单的用户界面，允许用户指定一个需要进行攻击的具体 IP、端口以及攻击持续的时间。填写完之后可以提交信息，页面上还包含了一句有意思的话：“不用对你的朋友使用它。”

他说，攻击者是一个高手，他使用了匿名代理 Tor 网络，用以隐藏他或者她的真实地址。

使用 Web 服务器来组建僵尸网络将比使用个人电脑拥有更大的带宽，因此，相比用个人电脑，它将能够使用更少的僵尸电脑来完成攻击，并且，使用 Web 服务器将减少被发现的几率，因为很少的 Web 服务器上会安装反病毒软件。

Shulman 说：“黑客可以使用一台服务器来取代 50 台电脑，从某种程度上而言，这种类型的攻击更具稳定性，因为它涉及到较少的电脑，同时它的攻击代码在僵尸电脑上被检测出来的概率也更低。”

当被问到发起这些攻击的动机时，Shulman 认为，很多 DoS 攻击都是用来勒索大量金钱，针对被攻击网站的所有者的。

“日本国防部被黑客攻击”疑似骗钱

来源：搜狐 it

9 月 20 日，瑞星公司发现，有人在天涯、百度贴吧等论坛发布“日本国防部网站被黑客攻陷”的帖子，在帖子里给出的网址链接是以“.jp”结尾的日本域名。但是，经瑞星安全专家检查发现，该网站不过是建立在日本免费网站上的一个个人主页，黑客用它来诱骗中国网民访问，凭借网站上的广告赚钱。

据介绍，近期以来随着中日钓鱼岛争端成为网民关注的焦点，有些不良黑客开始利用网民的心理来进行此类钓鱼式诈骗。他们通常在日本网站申请免费的域名和空间，在上面建立一个简单的攻陷页面，就去各大论坛发帖，号称自己攻陷了某某日本著名网站，其实是为了吸引网民去点击页面上的 Google 广告，从而获取收益。

目前尚未见到此类钓鱼式诈骗网站用来传播病毒，但从技术上讲，黑客完全可以在这些网站上植入木马病毒，以“日本网站攻击程序”的名义，欺骗网民下载安装。瑞星安全专家表示，近期用户在论坛、微博、贴吧等上面发现此类帖子，谨慎点击其中发布的所谓“日本网站网址”，因为那很可能就是病毒。同时用户也可以安装瑞星全功能安全软件 2011（测试版），其中集成有强大的反钓鱼和反挂马功能，可以有效阻止此类恶意网站的攻击。

瑞星安全专家介绍，往往黑客为表达爱国之情时，会通过涂改对方网站的形式，但挂入 Google 广告，借机赚钱的行为还比较少见。黑客成功入侵日本网站，也就意味着可以在被入侵网站中植入任何信息，包括最新病毒。

警惕黑客破坏网络安全

来源：搜狐 it

国内多省网络近来连续遭遇黑客攻击，造成危害。专家认为，黑客攻击低成本、低门槛、高利润，危害越来越大，亟需全社会高度重视，共同推动网络安全管理全面升级。

电信“黑客”

9月10日晚8时许，安徽不少地区的网民发现自己所用的电信网络出现异常：网络游戏、电影下载及QQ等聊天工具可以正常使用，但网页打开时却慢得出奇，最后显示“您指定的网页无法访问！”网络异常涉及合肥、阜阳、六安、巢湖等地，当晚10时半后，各地网络才恢复正常。

危害增大

记者了解到，黑客攻击事件愈演愈烈，无论其发生的频度还是广度，亦或是造成的危害，都呈逐年递增态势。

危害性也越来越大。2009年全国范围或省级行政区域内发生造成较大影响的网络安全事件较上一年增长，包括5·19我国六省区互联网网络故障事件、6·25中国电信广东省网流量异常事件、8月中下旬国际互联网海底光缆连续中断事件等，不仅给普通互联网用户造成较大或重大影响，还给相关部门和行业企业造成不少经济损失。

今年以来，北京、江苏、江西、广东、福建、安徽等地时不时出现黑客攻击事件。安徽省通信管理局互联网安全处负责人说，目前全省每个月都有不少网站被黑客侵扰。

管理漏洞

专家和业内人士认为，网络安全事件不断发生，暴露了我国网络管理的漏洞。

首先是应对黑客攻击技术层面的手段欠缺。“一方面，互联网的创新能力强，道高一尺魔高一丈，找出漏洞进行攻击总是比及时修复漏洞进行防御容易，所以黑客攻击事件在所难免，而且事后回溯很艰难；另一方面，互联网是个新生事物，如何有效抵御防范网络黑客攻击是一项系统庞杂的课题。”周峰说。

一些专家和业内人士认为，随着互联网普及，黑客手段呈公开化趋势。不仅黑客教材、网站随处可见，而且公开传授黑客技术，导致黑客犯罪成本小、门槛低，助长了黑客犯罪之风。“甚至一些不懂技术的网民也可以通过下载黑客软件搞破坏。”

有关专家建议，通过立法界定政府部门，以及运营商、应急组织、用户等环节的角色和定位，加大对黑客等不良信息的过滤，加大对攻击者的打击力度。

篡改 Comcast 网站黑客获刑 18 个月

来源：新浪

北京时间 9 月 25 日上午消息,据国外媒体报道,两名于两年前篡改美国有线电视运营商 Comcast 网站的黑客周五被判 18 个月监禁。

这两名黑客分别是 20 岁的克里斯多夫·刘易斯(Christopher Lewis)和 28 岁的迈克尔·内伯尔(Michael Nebel),他们都是电话黑客团伙 Kryogeniks 的成员,该团伙于 2008 年 5 月控制了 Comcast.net 网站。

在成功接管了一个用于控制 Comcast DNS(域名管理系统)信息的账户后,他们将用户重新定位到他们自己的网站,持续时间达数小时。当时的 Comcast.net 每天的独立用户访问量约为 500 万。

美国宾夕法尼亚州东部地区法院法官罗伯·特凯利(Robert Kelly)于周五对上述两名黑客进行了判决,他们还必须向 Comcast 赔偿 9 万美元的损失。

另外一名黑客詹姆斯·布莱克(James Black)则于上月被判 4 个月监禁。

近些年来发生的数起攻击事件暴露出 DNS 管理企业的安全问题。今年早些时候,百度也因为类似的攻击而无法访问。

在 Comcast 的攻击中,黑客利用社交工程技术欺骗用户向他们提供信息,从而借此访问了 Comcast 的网络解决方案 DNS 账户。

布莱克今年 3 月的供词显示,Kryogeniks 成员于 2008 年 5 月 27 日获得了网络解决方案账户的管理员权限,从而将 Comcast.net 的流量重新定位到他们自己的网站。

Comcast 为应对这一攻击共花费了 9 万美元。

委内瑞拉总统查韦斯 Twitter 账户疑遭黑客入侵

来源：中国新闻网

据外电报道,委内瑞拉内政部长塔里克·埃萨米(Tareck El Aissami)25 日表示,委内瑞拉总统查韦斯的 Twitter 账户疑遭到黑客入侵。

埃萨米说,自 9 月 22 日以来,查韦斯的 Twitter 账户出现混乱状况,至少 3 条微博都不是查韦斯本人写的。

埃萨米表示有人未经许可进入了查韦斯账户,目前经过修复,总统本人已经可以继续发布信息了。

委内瑞拉官员呼吁美国方面协助这一广受欢迎的社交网站管理员对此进行调查。

据悉,查韦斯在 Twitter 上有 85 万粉丝,每天会收到数百条留言。

黑客发动恶意攻击更具隐蔽性

来源：新华网

赛门铁克一名专家21日称，网络黑客正在不断变换手法向电脑用户发动恶意攻击，由于这些方法更具隐蔽性，所以防范难度越来越大。

赛门铁克软件安全部门经理约翰·哈里森对《科技新闻网》说，2000年，赛门铁克每天提供5个病毒签名，以应对恶意攻击。之后这一数字逐年攀升。到目前，赛门铁克每天提供的病毒签名高达2万至2.5万个。

根据哈里森的观点，目前网络恶意攻击呈现出以下新特点：

一、过去电脑用户只有在登录色情、赌博等不良网站时或使用盗版软件时才容易遭到恶意攻击，但现在不少旅游、购物和游戏等网站也成为黑客用来发动恶意攻击的平台。

二、过去的恶意攻击没有组织性，大多由不谙世事的年轻人所为，但现在的网络攻击不仅组织性高，而且专业性强，由不同的软件开发小组操控。

三、过去网络黑客往往通过传递邮件的方式发动恶意攻击，这种方式比较容易识别，但目前黑客是趁用户下载某些软件之际悄悄发动攻击，令用户难以识别。

四、黑客利用第三方的广告将恶意软件侵入用户系统，比如黑客会利用某个广告提醒用户，其系统已感染病毒，当用户根据广告提示去链接某个据说能杀病毒的网站时，这时“潜伏”在这个网站的恶意软件便会侵入用户系统。

五、黑客会设计用户信任的银行等网站的标识，当用户放松警惕登录这一网站时，便会遭到恶意软件的攻击。

哈里森还说，有迹象表明，今后黑客有可能会利用社交网站，向用户发送看似来自朋友或亲人的带病毒的邮件。

他说，网络安全部门要积极应对黑客，用户也应加强自我防范。

海外来风

One million malware-infected spam HTMLs appearing every day says Barracuda Networks

来源: scmagazineus 杂志

Hackers are using an increasing variety of sophisticated attack vectors to infect internet users PCs, and it seems that infected spam HTML is now being used as a carrier. In its latest attack vector analysis, Barracuda Networks claims that it is now seeing more than a million instances a day of unwanted emails containing malicious HTML attachments.

According to Dave Michmerhuizen, a security researcher with Barracuda Networks, hackers are trying every trick in the book, from using trending news topics to sending deliberately vague messages, in the hope that users will be curious enough to open the HTML.

"After all, what harm can an HTML file do?" he says, adding that the answer to this rhetorical question is: "plenty."

In his security blog, Michmerhuizen notes that users have been warned for years of the potential dangers associated with clicking on a file or link that arrives in an email. But, he says, many people assume that an HTML file is just a web page and that web pages are safe.

"This assumption is misleading", he said, adding that on September 16, one of the latest campaigns started with spam tied to current Google trending topic and which evolved over the next few days, with subject lines changing from trend topics to more non-specific email subjects.

The bad news, the Barracuda Networks' researcher says, is that the attachments include 100% obfuscated JavaScript which, when opened in a browser window, route users to sites such as fake video codec sites that include malware executables rather than codec plugins.

The problem with many obfuscated JavaScript attachments, says Michmerhuizen, is that the absence of any visual feedback means users have no idea what has just happened or that they have contracted one of the most dangerous pieces of malware (Zeus) on the internet.

"So yes, a seemingly innocent HTML email attachment can do plenty of damage, and while quite stealthy, definitely not harmless", he said.

博威特说：每天出现一百万个含有恶意软件的 HTMLs 邮件

来源：scmagazineus 杂志

——中国信息安全博士网翻译

黑客正在使用各种各样的更为先进的方式攻击互联网上的电脑，并且那些看似垃圾的 HTML 邮件现在正作为病毒的载体。根据最近的攻击载体分析，博威特公司声称，它现在看到一天超过一百万的实例含有恶意 HTML 附件的不明邮件。

据戴夫 Michmerhuizen，与博威特网络安全研究员，黑客正在试图利用每一个热点新闻主题，故意传送含糊的信息，促使用户有足够的好奇心，打开 HTML。

“毕竟，一个 HTML 文件能有什么伤害”他还补充说，对于这个问题答案是“肯定的”。

在他的安全博客，Michmerhuizen 注意到，用户已经被警告多年，打开那文件存在潜在的危险或者打开那邮件。但是，他说，许多人想当然地认为一个 HTML 文件只是一个网页，而网页是安全的。

9 月 16 日，他补充说：“这一假设是误导的”。最新的发现，垃圾邮件开始绑定谷歌搜索的热点话题并且预测未来数十天的。从不断变化的发展趋势主题，垃圾邮件开始更多的非特定的电子邮件主题。

博威特网络公司的研究人员说，坏消息就是 100% 的附件包括混淆的 JavaScript，在打开浏览器窗口时，用户在网站浏览，如假视频，包括恶意软件的可执行文件，而不是编解码器的编解码器插件的网站。

问题出在许多混淆的 JavaScript 附件，说 Michmerhuizen，通过任何视觉反馈用户没有发现刚刚发生的事情，或者他们在因特网上签约的是最危险的恶意软件作品。

“所以，那看似无辜的 HTML 电子邮件附件可以带来大量的破坏，虽然很隐蔽，但是绝对不是无害的”，他说。

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。

高端访谈下期预告：专访王昭顺教授

人物简介：王昭顺，男，1969 年 12 月生，浙江省淳安县人，汉族，教授，博士后，计算机系副主任。1993 年 6 月毕业于北京师范大学数学系，分别获理学学士和硕士学位。同年在北京科技大学计算机系工作，并于 2001 年 4 月开始担任计算机系副主任。1998 年 9 月在职攻读博士学位，于 2002 年 6 月获工学博士学位。2003 年 6 月在中国科学院研究生院信息安全国家重点实验室做博士后研究工作，并于 2006 年 4 月出站。

采访预告：

1. 首先，请王教授介绍一下北科大信息工程学院计算机系的情况（包括实验室的建设等）。
2. 从 1985 年开始，王教授用 8 年时间攻读数学系，1993 年硕士毕业，后决定转攻计算机，来到了北科大计算机系。（其实计算机与应用数学联系还是很密切的。但还是有一定的差别的。）在您决定转攻方向的时候，您的思想肯定是做了相当大斗争，您当时是怎样一个心态？
3. 我想每个人在人生中的抉择、困惑都会很多，最终的命运也是各不相同，到现在，您觉得您当初从数学转攻计算机的选择是正确的吗？有没有后悔？
4. 现在您主要研究哪些领域？
5. 在这些领域，您也陆陆续续有不少成果，在您眼中，“信息安全”这个词，我们怎么去诠释？
6. 您认为您研究的这三项领域都处在一个什么位置？它们之间有哪些联系？
7. 您研究过的许多成果，如：““蓝牙产品研发”和“蓝牙协议测试及相关技术开发”、“USB 密码钥匙漏洞分析及防御策略的研究”、“数字信封在智能卡对称密钥传输中的应用”、等等。这些研究成果也逐步运用到各个领域里，尤其是企业会多些，跟企业打交道频繁了，应该还是比较了解企业的，您认为，企业（我们这里就说信息安全企业）在选择项目时，对于企业本身的利益来讲，会考虑什么？
8. 您在和专家、博士等研发人员的合作上会有些什么要求？

企业推荐

广州市国迈科技有限公司

国迈科技是国内领先的移动存储介质安全专家和计算机内网安全专家。

国迈科技拥有一批承担过国家级火炬计划项目等重点项目的专家，和长期专注于计算机安全领域的资深研究员，在计算机、安全、通信三大领域都拥有深厚的知识积累和独到认识，具备强大的研发实力。

国迈科技占领技术制高点，参与制定了公安部公共安全行业标准、公安部公安信息网标准、保密局专用移动存储介质标准等多项重要标准，并通过了包括国家保密局、公安部、解放军保密委在内的多项权威认证。

国迈科技总部设在国家软件产业基地——广东软件科学园区，并且分别在北京、上海、佛山、湖南设有分公司。在武汉、成都、南京、杭州、西安、长沙、昆明、深圳、贵阳、福州、郑州、济南、石家庄、沈阳、哈尔滨、海口、乌鲁木齐等城市设有办事处。

公司提供积极的薪筹激励制度，以全方位的薪筹体系，鼓励员工与公司共同发展，并分享公司快速成长的喜悦。

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

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