

安全周报

中国信息安全博士网

六月 第四期
二〇一〇年六月二十五日

weekly.secdactor.com

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



SMP-U

国迈移动存储设备管理系统

唯一三证齐全的移动存储设备管理系统

U盘系统核心功能：

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

● 功能描述：

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

■ Internet告警中心：

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

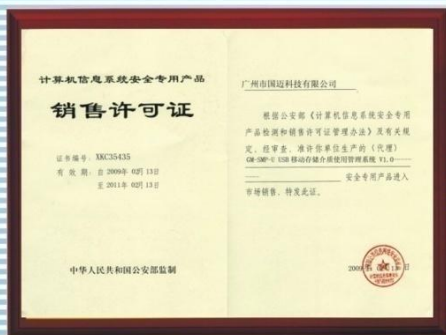
■ 专用安全U盘：

内部U盘、单向导入U盘、单向导出U盘、双向交换U盘。

权威认证：



国家保密局认证证书
ISSTEC2008YT0618



公安部认证证书
XKC35435



解放军保密委认证证书
军密认字第0587号

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

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

Guangzhou Goldmessage Technology Co., Ltd.



便携式计算机网络及 移动通信安全隐患展现系统

产品总述:

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

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

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

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

服务及时周到：为用户提供全面的技术支持与现场服务。

产品功能:

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

国工信科技发展（北京）有限公司

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



第三届中国信息安全博士论坛

(2010年7月31日-8月1日 宁夏·银川)



宁夏大学

欢迎您!

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

联合主办: 中国电子信息产业发展研究院
宁夏大学
北京电子科技学院

协办单位: 北京信息科技大学
北京交通大学
中国刑事警察学院

承办单位: 《信息安全与技术》杂志社
国工信科技发展(北京)有限公司

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

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

会议主题: 信息安全产、学、研的联盟创新与发展

会务组: 010-64126291 136611116129 张鹏飞

电子邮件: secdoctor@163.com

会议官网: meeting.secdoctor.com

目录

学术会议.....	7
第二届中国传媒与互联网高峰论坛 6 月 22 日举行.....	7
全国民族院校第三届教育信息化研讨会在北方民族大学召开.....	8
傲盾出席网络与信息安全技术工作委员会十次全会.....	8
2010 全球软件和信息服务高层论坛暨企业家峰会	9
政府之声.....	10
美国拟推出防黑客新法 奥巴马有权关闭因特网	10
工业和信息化部举办 2010 年中央国家机关信息安全培训班.....	10
信息安全协调司组织召开政府部门互联网安全接入试点工作会议.....	11
四川省首个地市级信息安全测评中心攀枝花分中心正式成立.....	12
罗江供电局开展计算机信息安全专项检查.....	13
病毒播报.....	13
暑游升温 诸多旅游类网站引发黑客攻击.....	13
国家计算机病毒应急处理中心病毒预报（2010.6.19-2010.6.25）	14
冠群金辰 6 月第 3 周病毒报告：病毒数量下降.....	15
Yonsole 病毒致 Windows 系统黑屏无法启动	18
江民科技 06 月 23 日病毒播报：“埃德罗”变种 jlg 和“毒疤”变种 wmx.....	19
利用小女孩及其母亲 僵尸网络钓鱼网银.....	21
世界杯第一高危木马爆发 “呜呜祖拉”下载器感染 420 万电脑.....	22
“苍井空现象”诱发不良木马攻击剧增	24
产业动态.....	25
网游反盗号告别单打独斗 切断隐秘利益链条.....	25
360 安全卫士争端.....	27
世界杯火爆 Twitter 宕机 SNS 需要投怀云计算？	31
谷歌收购 AdMob 细节:5.3 亿股票加 2.2 亿美元现金.....	33
杭州首例非法获取公民个人信息案一审宣判	34
思科升级云安全平台 推电子邮件与 Web 安全服务	34
赛门铁克发布最新月度安全报告	35
360 微博回应搜狗浏览器网速保护被报木马	36
两成 Andriod 应用程序存在安全威胁.....	37
技术前沿.....	37
云安全联盟（CSA）公布云安全七宗罪	37
从 C.I.A 三性看云计算的数据安全.....	38

IT 发展趋势驱动全新安全方法	42
熊猫安全:真云不怕“毒”炼.....	43
域名注册机构采用.org 最新安全性措施.....	44
专家为你解读 高校 Web 安全“新药方”	45
安全远程访问: 为企业应变计划填补空缺.....	47
云端安全: 可信任的云计算前端让性能可靠	49
黑客攻防	51
苹果偷偷发布补丁修复一个木马安全漏洞.....	51
安全厂商常漏掉新恶意软件.....	52
内部用户帐户控制: 谁来监督“监督人员”?	52
Wi-Fi 加密技术屡屡遭破	53
数据丢失防护部署中的五大安全技巧.....	54
21 世纪经济报道: 信用卡存危险盗刷暗门.....	55
企业推荐.....	60
艾特赛克(北京)信息技术有限公司.....	60

学术会议

第二届中国传媒与互联网高峰论坛 6月22日举行

来源：新浪科技

为加快传统媒体向跨媒体、新媒体、全媒体转型，更广泛深入地应用以软件开发为核心的数字、互联网新技术，由大连软交会组委会主办、市政府和中国报业网承办的第二届中国传媒与互联网高峰论坛昨日在大连世界博览广场举行。作为第八届大连软交会的一项重要内容，此次论坛的主题是“融合、创新、力量”，并且首次推出创新媒体展，旨在搭建传媒与数字技术、互联网软件交易的平台。中宣部原常务副部长龚心瀚，市委常委、副市长戴玉林出席了开幕式。

互联网的出现帮助人们彻底突破了信息传播媒介和时空的障碍，其海量、便捷、高效和互动性深入人心，越来越多的人正逐渐改变获取信息的方式和习惯，网络电视、视频网站、手机报、手机电视、移动电视、电子阅读器等以互联网与信息技术为基础的新媒体越来越多地成为人们生活、娱乐、学习、工作、沟通、交友等方面不可或缺的工具。年轻一代逐渐远离传统电视和报刊的趋势越来越明显，传统媒体的生存和发展受到了巨大的威胁，面临着巨大的挑战。因此，第二届中国传媒与互联网高峰论坛顺应新传媒、新技术、新营销的发展趋势，特别邀请全国领先的主流媒体、领先的新媒体企业、领先的技术服务商和战略投资公司以实战合作的方式，共同探讨传统媒体战略转型的紧迫性、必要性、成长路线、商业模式和投资价值。来自传统媒体、跨媒体集团、无线新媒体、网络媒体、户外新媒体、互联电视制造商、数字出版运营商、传媒研究机构和新媒体艺术院校等单位代表近百人参会。与会专家围绕传统媒体与网络媒体的合作、传媒业的数字化趋势、报纸网站盈利模式、数字媒体营销等议题，进行了深入而广泛的交流。

借第八届软交会的东风，本届高峰论坛首次推出的创新媒体展，演绎了媒体与数字技术的精彩结合，展示了网络新媒体、手机报、数字出版、电子阅读终端产品、视频网站和数字化媒体软件及解决方案等。同时，本届论坛还将举行“总编辑大连软件产业行”，数十家全国主流报纸、网站的总编辑将参观大连软件产业，品读大连具有世界影响力的软件文化。

全国民族院校第三届教育信息化研讨会在北方民族大学召开

来源：北方民族大学

6 月 18 日-19 日，全国民族院校第三届教育信息化研讨会在北方民族大学召开。来自中央民族大学、西南民族大学、中南民族大学、西北民族大学、北方民族大学、大连民族学院、西藏民族学院、贵州民族学院、青海民族大学 9 所民族院校和宁夏区内高校的 50 多位代表参加了会议。副校长杨敏出席会议并致开幕辞。

本届研讨会以“民族高校教育信息化建设与应用”为主题，通过专题报告、座谈交流、分组讨论等形式，就民族院校现代教育技术应用现状与发展，网络建设，新技术、新方法、新设备的引进等方面情况进行了交流，并就民族高校数字化校园的规划、建设、实施，资源、数据共享等信息化建设中的热点问题进行了深入探讨。

此次会议的召开，对推进全国民族院校教育信息化建设具有积极促进作用。

傲盾出席网络与信息安全技术工作委员会十次全会

来源：比特网

2010 年 6 月 12 日，中国通信标准化协会网络与信息安全技术工作委员会(TC8)第十次全会在北京友谊宾馆召开，傲盾公司作为企业代表应邀出席了会议。

会议由 TC8 主席方滨兴院士主持，副主席刘辛越教授、通信标准化协会武冰梅副秘书长等领导出席了会议。会议听取了 TC8 主席方滨兴院士的 2010 年上半年工作总结及各工作组组长的工作报告，讨论通过了 TC8 各组新完成的标准、技术报告和 2010 年第一批立项建议。

2002 年 12 月，中国通信标准化协会在“通信安全标准研究组”基础上成立“通信信息安全技术工作委员会”。2003 年 6 月，经部科技司、电信管理局、中国通信标准化协会研究决定，将原定名“通信信息安全技术工作委员会”改为“网络与信息安全技术工作委员会”。中国通信标准化协会一贯遵照公平、公正、公开的原则制定标准，并进行标准的协调、把关，旨在把高技术、高水平、高质量的标准推荐给政府、企事业单位。其会员单位加入标准高、审核程序严格，在业内极具权威性。

傲盾是一家已有十二年发展历史，并且正在高速成长的公司，作为国内领先的互联网产品与解决方案提供商和信息网络安全产品与解决方案提供商，傲盾一直致力于持续的技术研究和技术创新，并坚守“安全防护，傲盾先行”的公司理念和“技术为本，与客户共同成长”的公司愿景。2010 年 3 月，傲盾加入了 TC8，成为其全权会员单位，同时拥有四个工作组的参会、议会和标准制定资格。

2010 全球软件和信息服务高层论坛暨企业家峰会

来源：比特网

以“实现两化融合，创造绿色增长”为主题的第八届中国国际软件和信息服务交易会于 6 月 22 日在大连拉开序幕，作为软件行业最具盛名、影响力最广泛的会议，吸引了来自全球各个国家和地区的政要和企业代表。据悉，本届展会以“软件创造绿色增长”为主题，划分为国际合作、软件创新、行业应用、资金对接、人才交流、信誉保障六大板块，由展览、会议论坛、重要活动三个组成部分。

现场发现，跨国公司组成了独特的“跨国公司走廊”，囊括了 IBM、思科、麦肯锡、惠普、微软、甲骨文、埃森哲、简柏特、NIIT、富达基金、花旗、戴尔等 35 家知名软件、IT 服务、咨询企业巨头，相比，国内软件企业同样引人瞩目，包括自家地盘上的东软集团，联想、用友、中科红旗、方正、启明信息、浙大网新、文思创新、环宇、华录、海辉、华信、安博教育等，甚至连中国移动、中国联通、中国电信三大运营商也排出了强大阵容。

6 月 22 日至 25 日为软交会展览期。其中 6 月 22 日为主论坛及展览开幕日。展会期间还将举办“软件创新、服务外包、产业趋势、版权保护、项目管理、工程创新”六个方面的主题论坛。其中“IT 项目管理论坛”和“工程创新论坛”是今年首次举办。此外还将举行系列行业会议，以及部分企业、地方政府组织、行业协会的各类会议论坛等共计 50 余项，80 多场次。

记者从软交会组委会获悉，今年在软交会期间举行的区域交流、推介活动明显增多。珠三角、长三角、东北地区、中原地区等地省市政府都希望通过软交会与大连沟通交流，软交会期间，河北省、无锡市、郑州市等还将举办专门的软件与服务外包产业推介会，期望在软件产业中开创出新的天地。

大连市委常委、副市长、第八届中国软交会组委会秘书长戴玉林透露，本届大会第一个亮点是国内省市组团踊跃。今年有来自除西藏外的 30 多家省市组团参展，大连软交会在全国省市心目认可度持续提高；第二大亮点是世界五百强企业参展数量再创新高；第三个亮点是中国软交会积极主动与多行业融合，今年有通讯、金融、医疗、教育、财务、保险等近三十个行业在中国软交会上与多行业寻找融合机会，各种行业到软交会上寻找新的技术，寻找新的思维，寻找各类人才。

作为曾连续举办八届软交会，规模、规格不断提高的东道主，大连市入驻的世界 500 强企业从 2001 年的 3 家增加到目前的 53 家，发展迅速。在 2009 年，大连市新增软件和信息服务业从业人士多达 8000 人，获取国家补贴 3600 万元，已连续第四年获取国家相关补贴金额第一位。从海关报关统计来看，大连也一直在国内各城市中蝉联软件出口第一位。目前，国内包括大连、无锡等城市均在大力发展软件外包等业务，但也仅占全球软件外包市场的 5%。

据第八届中国国际软件和信息服务交易会组委会介绍，作为目前国内最高规格、最具实效和最具国际影响力的 IT 行业展会，大连软交会愈来愈受到国内外各界人士的广泛关注和普遍认可，成为

中国软件和信息服务产业发展的风向标。尤其是伴随着我国工业化和信息化的深度融合，信息化日益成为改变未来各行业走向的最重要指标，软件产业与传统工业间的结合越来越紧密，为两化建设注入新鲜血液和活力。

政府之声

美国拟推出防黑客新法 奥巴马有权关闭因特网

来源：中国新闻网

中新网 6 月 21 日电 美国一项新法案将赋予总统奥巴马权力，于“国家紧急事态”下关闭因特网。据香港《文汇报》报道，法案一旦通过，奥巴马将有权命令 Google 和雅虎等受欢迎网络搜寻器暂时关闭，其他美国网络服务和宽频供应商也须遵从，违例将面临巨额罚款。

法案由前总统参选人、参议院国土安全委员会主席利伯曼提出，但遭到美国最大科技游说组织 TechAmerica 批评，指法案让白宫“拥有潜在绝对权力”和“滥用权力”。

然而，国家情报总监布莱尔年初曾指出，美国正受“恶意网络攻击严重威胁”，政府部门网络过去 3 年的受袭次数上升 400%。

根据法案，任何被国土安全部列为“依赖”因特网、电话系统或是任何美国“信息基建”的公司，都将受国安部内新设的国家网络保安及通讯中心指挥。

工业和信息化部举办 2010 年中央国家机关信息安全培训班

来源：信息安全协调司

为落实中央领导同志关于加大信息安全教育工作力度的重要批示精神，加强信息安全培训，促进提高中央国家机关各部门信息安全管理业务水平，工业和信息化部 6 月 8 日至 11 日在云南昆明举办了 2010 年中央国家机关信息安全培训班。来自国务院部委及直属机构共 69 个单位的 79 名信息安全处长及相关技术、管理人员参加了培训。工业和信息化部信息安全协调司赵泽良司长出席培训并做了动员讲话。

此次培训班重点培训信息安全最新形势、技术发展趋势、信息安全管理、信息安全检查、信息安全最新实践等方面的内容。北京邮电大学校长方滨兴院士、安全部吴世忠局长、国家密码局冯登国副局长、公安部科技信息化局马晓东总工程师等专家学者分别为学员进行了认真授课。

学员们普遍反映,通过本次培训对国家信息安全总体形势、技术发展趋势有了更深刻的认识,对相关政策文件有了更准确的把握,提高了做好信息安全工作的知识与技能,同时希望工业和信息化部加强培训工作力度,进一步支持各部门信息安全工作。本次培训得到了云南省工信委、工信部电子科学技术情报研究所的大力支持和协助。

信息安全协调司组织召开政府部门互联网安全接入试点工作会议

来源: 信息安全协调司

为总结政府部门互联网安全接入试点阶段性工作,推广应用试点工作成果,研究部署下一阶段试点工作,经工业和信息化部领导批准,信息安全协调司于2010年6月18日至19日在上海市青浦区组织召开了政府部门互联网安全接入试点工作会议。信息安全协调司赵泽良司长、杨春艳副司长,上海市经济和信息化委员会陈跃华副主任,上海市青浦区李跃旗副区长出席会议并讲话。全国信息安全标准化技术委员会委员曲成义、国家信息中心首席工程师孙大奇、国家信息技术安全研究中心总工程师李京春、信息安全共性技术国家工程研究中心副主任李嵩等政府部门互联网安全接入试点工作专家指导组专家参加了会议,并对安全接入试点工作给予技术指导。

会议听取了北京、上海、重庆、陕西等试点地区情况汇报,现场观看了上海市青浦区政府部门互联网安全接入和集约化管理演示。青浦区通过归并整合区政府部门互联网接入口,统一部署技术防范措施,实施办公用计算机终端管理,实现了全区110多家政府部门集中接入互联网,切实增强了政府部门的信息安全防护水平。

会议经过讨论认为,在专家的指导下,经过试点单位的积极探索和不懈努力,试点工作取得积极进展。试点工作实践证明,缩减政府部门互联网接入口数量,实施集约化安全管理,提高与互联网相连的政府信息系统安全防护水平在技术上是可行的,既可以提高安全可控水平,又降低了建设和管理成本。会议要求,应把政府部门互联网安全接入作为做好政府部门信息安全工作的重要切入点,切实推动。已开展试点工作的单位要进一步扩大试点工作的广度和深度,做好成果推广;下一阶段将开展试点工作的单位要注重借鉴已有工作成果,按照分类指导、分步实施的原则稳步推进。要尽快制定完善相关规范,为全面开展政府部门互联网安全接入工作提供标准依据。

北京、天津、河北、黑龙江、上海、重庆、云南、陕西、新疆生产建设兵团等地区工业和信息

化主管部门负责信息安全工作的领导和有关同志约40人参加了会议。

四川省首个地市级信息安全测评中心攀枝花分中心正式成立

来源：攀枝花市电子政务建设管理中心

四川省信息安全测评中心攀枝花分中心授牌仪式在攀枝花会展中心举行。市委常委、市委书记、市信息化工作领导小组副组长邵革军出席成立仪式并讲话。省经信委党组成员、省信息化工作办公室副主任李建疆到会致辞。会议由市政府秘书长、市信息化工作领导小组副组长贾德华主持。攀枝花市相关部门近 200 人参加了授牌仪式。



攀枝花市作为目前四川省信息化程度较高的市州之一，信息技术应用的逐步深入，伴随而来的信息安全威胁也日益突出，加强信息安全成为攀枝花市信息化建设工作的重中之重。经过攀枝花市一年多的努力争取，四川省信息安全测评中心决定在攀枝花市成立分中心，该中心成为四川省首个地市级信息安全测评中心。

攀枝花市信息安全测评中心主要承担政府信息网络、重要信息系统的安全测试与风险评估，开展信息技术产品、系统和工程建设的安全性测试与评估，从事信息安全测试评估的理论研究、技术研究等。此次在攀枝花市建立信息安全测评分中心，大力提升了攀枝花市信息化建设在信息安全保障的能力，标志着攀枝花市信息化建设水平迈上了一个更高的台阶。

罗江供电局开展计算机信息安全专项检查

来源：四川新闻网

四川新闻网德阳6月23日讯（曾杰） 今上午，冒着小雨，罗江供电局班子成员带队分赴基层班组专项检查计算机信息安全情况，宣贯德阳电业局22日公布的《关于对计算机违规外联行为处罚的暂行规定》。

6月上旬，罗江局曾经发生两起违规外联行为，当时就引起了该局对信息安全工作的高度重视。事件发生后，该局除对违规外联责任人进行教育处罚外，还再次明确了信息安全工作的分管领导和责任部门、责任人员，落实了各项信息安全管理度。同时，通过事件在全局员工中开展了一次反思教育，并采取了全员签定信息安全责任书，对内网工作用计算机进行清理，组织员工深入学习信息安全知识，提升信息安全管理手段，严肃信息安全纪律和制度等五项措施。

此次，针对再次发生的十余起违规外联行为，德阳局公布实施了新的《计算机违规外联行为处罚暂行规定》。为尽快宣贯这项新规定，6月23日早会后，罗江局召开了计算机信息安全工作会。会后，该局领导班子成员分别带队到各科室班组、供电所、多经公司和控股公司检查计算机信息安全情况和宣贯新规定。

据悉，在当天的检查和宣贯活动中，该局各检查组通过组织员工召开会议宣贯电业局新规，全面检查基层班组计算机软硬件使用情况，清理笔记本电脑等方式，使全局员工认识到了信息安全的重要性和违规外联的严重后果。该局部份员工表示：“处罚1000元，待岗一个月，还得去警示教育室参加学习，最主要的是影响全局的绩效，这样的外联违规成本太高，今后一定管好自己，并随时提醒身边的同事不违规。”

病毒播报

暑游升温 诸多旅游类网站引发黑客攻击

来源：千龙网

金山毒霸云安全监测中心近日截获了多组，以提供“暑期出游”查询、票价在线购买的恶意网址，网址诱骗用户点击后，篡改用户系统和浏览器设置，用户若未安装专业安全工具，极易遭受病毒侵袭。

据悉，近日伴随高考结束，高三学子们耗时三年之久的艰难备考期也划上句号，暑期旅游成为

很多考生走下考场放松心情的首选。“作为最后一个高中暑期，我和很多同学一样也都选择在高考结束后与家人出游，”来自北京的高三考生刘旭告诉记者，“通过网上很多旅行社的暑期推荐，东南亚成为最后确定要去的目的地。”

但刘旭在浏览了一些提供旅游地区查询、打折机票购买类网站后，刘旭发现自己的电脑就出现了很多问题，如自己的浏览器主页也被篡改了、莫名增加多个 IE、操作系统插件等，后经朋友推荐，使用金山卫士等专业安全工具进行扫描，发现显示查杀出多个木马病毒。后安装金山网盾等防护工具重新浏览相关站点，也被提示其为恶意网站。

对此，金山毒霸安全实验室反病毒专家李铁军解释道，一些恶意软件传播者正是抓住了高考后考生旅游热的热点，开始利用旅游类网址大肆传播木马病毒。据金山毒霸云安全实验室统计数据显示，一些知名旅游网站都存在恶意网址，极易蒙骗用户点击，在高考结束的两周时间里，针对旅游出行类网址相关的挂马、钓鱼网站也一直处于上升趋势。

金山毒霸安全实验室反病毒专家李铁军建议网民，网上搜索“暑期旅游推荐”、“特价机票查询”等相关信息时，应小心识别查询网站，避免误入挂马网站或者钓鱼网站。他指出，网页挂马从技术上已经完全可以实现很高的拦截率，网民只要安装金山网盾类的防护工具就可以大大降低上网浏览网页时的中毒风险。

同时，专家提醒，部分木马病毒会在诱骗用户点击相关恶意网址后，利用操作系统和浏览器漏洞进行传播，对此，李铁军同时建议网友，安装金山卫士等提供漏洞修补的工具，及时下载更新系统补丁，有效确保系统安全，避免因电脑中招而影响到暑期的出行心情。

国家计算机病毒应急处理中心病毒预报（2010.6.19-2010.6.25）

来源：国家计算机病毒应急处理中心

国家计算机病毒应急处理中心通过互联网络监测发现，微软公司在发布了 6 月一系列漏洞补丁程序之后，又曝出一个 HCP 协议漏洞，即 HCP 协议“零日”漏洞，该漏洞仅影响 Windows XP 和 Windows 2003。一旦计算机用户使用浏览器 IE（只针对 IE 版本 6.0）打开一些被挂马的 Web 网页，或是利用播放软件运行“染毒”的音频文件时，操作系统会自动弹出系统中的“帮助和支持中心”，并自动下载运行其他的病毒、木马等恶意程序，从而使操作系统被恶意攻击者任意远程控制。

HCP 协议，类似于 HTTP 之类的协议，它可以通过资源定位器 URL 的链接来开启“帮助和支持中心”功能。“帮助和支持中心”（HSC）是 window 中的帮助功能，可提供类似是否需要下载安装更新软件等各种帮助。操作系统中的浏览器 IE 在默认情况下可以利用该协议将“帮助和支持中心”打开的。如果计算机用户访问了受到 HCP 协议漏洞攻击的挂马 Web 网页，那么恶意攻击者预先设定的恶

意脚本程序文件将被自动运行，同时会自动打开 Windows “帮助和支持中心”，最终导致恶意木马程序入侵感染操作系统。

除挂马网页外，恶意攻击者还可以把 HCP 协议漏洞攻击代码嵌入到一些高级音频媒体文件中，当计算机用户打开这些已经嵌入代码的媒体流文件时，操作系统同样会受到恶意木马程序的入侵感染。

截至目前，微软公司在其官方网址上已经发布存在 HCP 协议漏洞的信息，其安全编号是 2219475，网址为：www.microsoft.com/technet/security/advisory/2219475.mspx，但并未透露何时发布官方漏洞补丁程序。

专家提醒：

对上述情况，我们建议广大计算机用户采用如下方法防范：

（一）针对已经受恶意木马程序入侵感染的计算机用户，建议立即升级系统中的防病毒软件，进行全面杀毒。

（二）针对未受到恶意木马程序入侵感染的计算机用户，我们建议暂时手工关闭操作系统的 HCP 功能，在微软公司发布漏洞补丁后再重新开启该功能。与此同时，打开系统中防病毒软件的“系统监控”功能，从注册表、系统进程、内存、网络等多方面对各种操作进行主动防御，这样可以第一时间监控未知病毒的入侵活动，达到全方位保护计算机系统安全的目的。

冠群金辰 6 月第 3 周病毒报告：病毒数量下降

来源：比特网

本周总体病毒状况继续保持相对平稳的状况，未出现严重的病毒及网络安全事件。受端午小长假的影响，一周总的捕获样本数量较前一周有所下降。

本周的常见病毒种类主要以网游盗号类/信息盗窃类木马程序(win32/gamepass 家族、Win32/wowpa 家族)、downloader 变体(Win32/silly 家族)、QQ 盗号类木马为主，新出现的变体数量也呈下降趋势。由于近期没有出现较易利用的新漏洞，因此近期黑客主要利用的漏洞相关的病毒变化不大，较常见的都是比较老的系统漏洞：

JS.CVE-2008-0015exploit - Microsoft Video ActiveX 漏洞(本周比较突出)

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

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

JS.MSDirectShowexploit - 利用 Directshow 漏洞;

本周关注病毒：

病毒名称: Win32.Gamepass Family 网游盗号木马家族

病毒别称: Troj/KbdSpy (Sophos), TROJ_KEYSPY (Trend), PWS-OnlineGames (McAfee)

病毒属性: 特洛伊木马

危害性: 中等危害

病毒特性:

Win32/Gamepass Family 病毒变体很多, 在 2008 年至今一直是较为常见的木马病毒。这个家族的变体繁多, 变化很快, 流传面积也较广泛。它们都是针对网络角色扮演类游戏制作的盗号类木马。此家族的病毒文件大多使用以下外壳打包自身: UPX, UPack, FSG 和 NSAnti。

这个病毒主要针对如下网络游戏(从游戏的流行程度看, 这个家族病毒主要针对国内和亚洲地区):

AskTao 《问道》

Nexia the Kingdom of the Wind

MapleStory 冒险岛

Dungeon & Fighter 地下城与勇士

Fantasy Journey Online

The Warlords 军阀

World of Warcraft 魔兽

Perfect World

Yulgang (Scions of Fate)

Legend of Mir II

Lineage II

根据不断跟踪, 此类盗号木马估计是由专门进行网络游戏盗号的团体进行制作/维护。主要通过盗取网络游戏玩家的游戏装备牟利。本周捕获大约 5 种变体, 请广大游戏玩家注意及时升级自己的反病毒特征库。

感染方式:

这个家族的大部分变体通过网页挂马方式传播, 部分通过其他木马下载器传播。当病毒文件被感染者执行后, 将搜索系统中对应的游戏窗口, 对用户的帐号、游戏配置等信息进行记录转发。

危害:

此病毒被执行后会监视现有系统进程名称和打开的窗口名称, 检查是否有以上针对的游戏程序正在运行中。它还会在系统中安装一些通用挂接 dll 库, 用以对键盘/鼠标的输入截取。当用户登录游戏后, 关键的帐户信息会被记录下来。

除此之外, 病毒还会记录下被感染系统的一些其他情况, 例如: 系统 ip 地址、游戏服务器的名称、游戏中的任务角色或者等级、游戏的地图细节等。

最后, Gamepass 将这些收集的信息保存到自己的日志文件中, 然后发送给远程的攻击者, 而且有些变体会通过邮件或者 web post 的方式发送到攻击者的网站。

本周常见病毒类表:

	Role Playing Game (MMORPG) "World of Warcraft" 游戏相关的用户名和密码。
JS/CVE-2010-0249!exploit	IE 极光漏洞利用脚本
JS.CVE-2010-0806exploit	IE 漏洞利用脚本;
JS.MSDirectShowexploit	微软 DirectShow 漏洞类脚本, 通常为挂马病毒使用。
Win32.OnlineGame!generic	盗号木马类
Win32.Sality.AK	是一种多形态病毒, 感染 Win32 PE 可运行程序
W Win32.VBDoor.BR	后门类程序, 部分变体使用 MS-VB 编写
Win32.Lolyda.HK	网游盗号类木马
Win32.Patchload	下载器类蠕虫 木马;
Trojan.Win32.StartPage	修改 IE 等浏览器主页的木马程序;

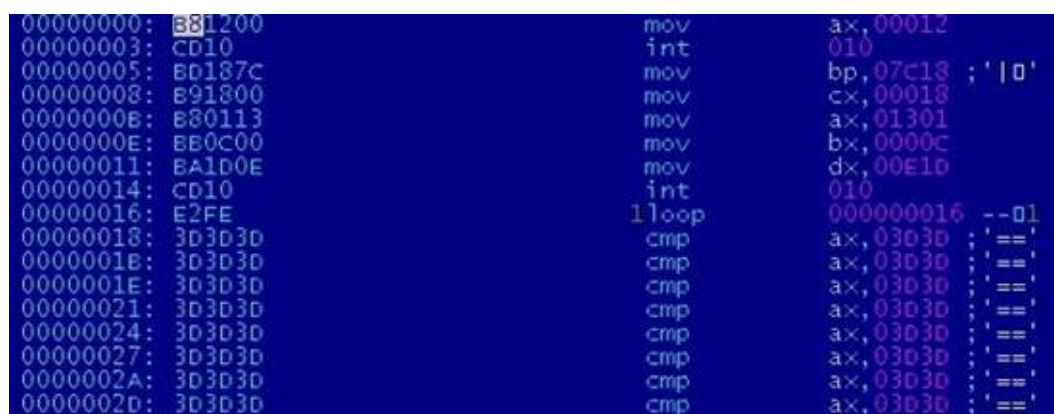
病毒名称	特性
GIF.Iframe!generic JPEG.IFrame!generic	在网页的图片尾部加入 js 脚本代码, 利用 IE 漏洞执行其中的脚本;
Win32.GameThief.F	近期最常见的木马程序也是数量最多的家族, 本周共捕获 2 种变体;
Win32/Gamepass	近期最常见的木马程序也是数量最多的家族, 本周共捕获 6 种变体;
Win32.Zuten!generic	盗取在线游戏的木马;
Win32.Wowpa	此家族属于记录按键的木马程序, 它一般是被其它恶意软件安装。它尝试盗窃与 Massively Multiplayer Online

Yonsole 病毒致 Windows 系统黑屏无法启动

来源：驱动之家

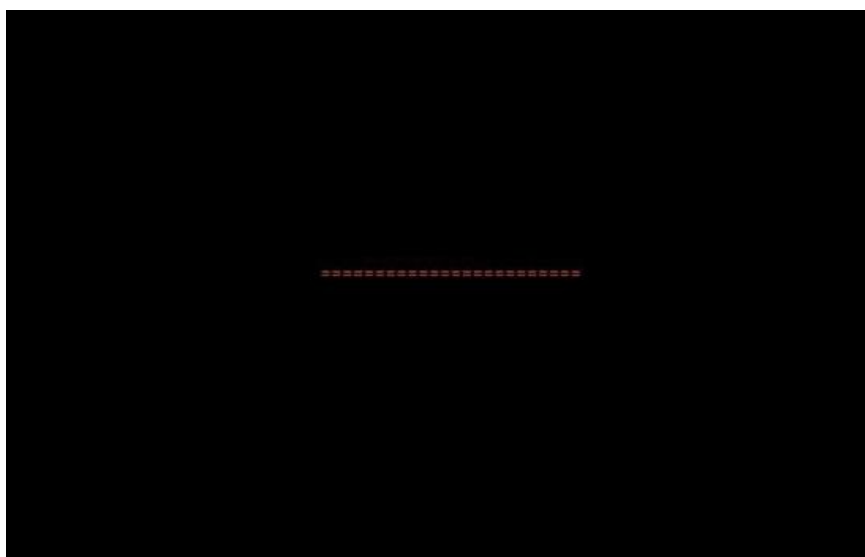
微软日前表示，一种新的恶意软件将破坏 Windows 启动进程，阻止系统启动。微软检测到的这个木马病毒为 Backdoor:Win32/Yonsole.A，受感染的计算机会受到攻击者的远程控制，执行各种指令。

微软安全人员 Chun Feng 解释说：“这个最近发现的后门程序可以接受并执行远端服务器的指令，修改受感染计算机的主引导记录（MBR）。它对 MBR 的修改十分类似于‘Stoned’病毒对 DOS 的修改。不同的是，受 Yonsole 感染后，MBR 只在屏幕中间显示一道虚线，并且不再启动。我们将新的 MBR 检测为 Trojan:DOS/Yonsole.A。”



```
00000000: 381200      mov     ax,00012
00000003: CD10        int     010
00000005: BD187C      mov     bp,07c13 ;'|0'
00000008: B91800      mov     cx,00018
0000000B: B80113      mov     ax,01301
0000000E: BB0C00      mov     bx,0000C
00000011: BA1D0E      mov     dx,00E10
00000014: CD10        int     010
00000016: E2FE      iloop   000000016 --dl
00000018: 3D3D3D      cmp     ax,03D3D ;'=='
0000001B: 3D3D3D      cmp     ax,03D3D ;'=='
0000001E: 3D3D3D      cmp     ax,03D3D ;'=='
00000021: 3D3D3D      cmp     ax,03D3D ;'=='
00000024: 3D3D3D      cmp     ax,03D3D ;'=='
00000027: 3D3D3D      cmp     ax,03D3D ;'=='
0000002A: 3D3D3D      cmp     ax,03D3D ;'=='
0000002D: 3D3D3D      cmp     ax,03D3D ;'=='
```

MBR 代码



启动屏幕

受此病毒感染后，用户将无法控制自己的计算机，攻击者则可以远程执行各种命令。微软表示：“Backdoor:Win32/Yonsole.A 会将自己植入 services.exe，并下载一个 DLL 文件到，比如 f00165500k.cmd，这个 DLL 文件包含后门功能，可能被检测为 Backdoor:Win32/Yonsole.B。Backdoor:Win32/Yonsole.A

将下载的 DLL 文件作为 Service DLL 安装到计算机上，以确保每次 Windows 启动时都会加载。”

Yonsole 影响很多 Windows 版本，包括 Windows 2000 和 Windows NT：将 DLL 文件放到 C:\Winnt\System32 中；Windows XP、Windows Vista、Windows 7：将 DLL 文件放到 C:\Windows\System32 中。

江民科技 06 月 23 日病毒播报：“埃德罗”变种 jlg 和“毒疤”变种 wmx

来源：计世网

英文名称：TrojanDownloader.Adload.jlg

中文名称：“埃德罗”变种 jlg

病毒长度：53760 字节

病毒类型：木马下载器

危险级别：★

影响平台：Win 9X/ME/NT/2000/XP/2003

MD5 校验：54f91c39aa649409327374f55cb943c5

特征描述：TrojanDownloader.Adload.jlg “埃德罗”变种 jlg 是“埃德罗”家族中的最新成员之一，采用“Microsoft Visual C++ 6.0”编写，经过加壳保护处理。“埃德罗”变种 jlg 运行后，会在被感染系统的“%SystemRoot%\system32\”和“%SystemRoot%\system32\dllcache\”文件夹下分别释放恶意 DLL 组件“dxuc1.dll”，还会在“%SystemRoot%\system32\”文件夹下释放“dxucf.dll”、“ggsss7.dll”。释放完成后，原病毒程序会释放批处理文件“3750540.bat”并调用运行，以此将自身删除。“埃德罗”变种 jlg 会在被感染计算机的后台遍历当前系统中运行的所有进程，一旦发现“ravmond.exe”和“360tray.exe”存在，便会尝试将其结束，从而达到自我保护的目的。“埃德罗”变种 jlg 运行时，会在后台访问骇客指定的站点“www.love*580.cn”，从而提高了指定站点的访问量。秘密连接骇客指定的站点 221.194.*.33:80，侦听骇客指令，在被感染计算机上执行相应的恶意操作。骇客可通过“埃德罗”变种 jlg 完全远程控制被感染的计算机系统，致使用户的计算机安全和个人隐私面临着严重的侵害。另外，“埃德罗”变种 jlg 会将释放的“ggsss7.dll”注册成 BHO（Browser Helper Object，浏览器辅助对象），以此实现指定恶意文件开机自动运行的目的。

英文名称：Trojan/Scar.wmx

中文名称：“毒疤”变种 wmx

病毒长度：40960 字节

病毒类型：木马

危险级别：★

影响平台：Win 9X/ME/NT/2000/XP/2003

MD5 校验：0e4df0725b69b855efa9665a319fcdfa

特征描述：Trojan/Scar.wmx “毒疤”变种 wmx 是“毒疤”家族中的最新成员之一，采用高级语言编写，经过加壳保护处理。“毒疤”变种 wmx 运行后，会自我复制到被感染系统的“%SystemRoot%\system32\”文件夹下。不断尝试与控制端（IP 地址为 204.45.*.110:80）进行连接，如果连接成功，则被感染的计算机就会沦为傀儡主机。骇客可以向被感染的系统发送恶意指令，从而执行任意控制操作（其中包括：文件管理、进程控制、注册表操作、服务管理、远程命令执行、屏幕监控、键盘监听、鼠标控制、音频监控、视频监控等），致使被感染系统的用户面临着严重的威胁。另外，“毒疤”变种 wmx 会在被感染计算机中注册名为“Wafter Comennection Driverr”的系统服务，以此实现开机自动运行。

针对以上病毒，江民反病毒中心建议广大电脑用户：

- 1、请将江民杀毒软件升级至最新版本，并且进行全盘扫描。江民杀毒软件增强了虚拟机脱壳与启发式扫描技术，能够更加轻松地识别各种加壳、家族变种病毒，使病毒无所遁形。同时应用指纹加速、超线程扫描等高速扫描技术，更好更快地保护您的信息安全。
- 2、江民网络版的用户请及时升级控制中心和所有客户端，并且进行全网的病毒查杀，最大程度地保障企业的信息安全。
- 3、开启江民杀毒软件的主动防御功能。该功能采用智能沙盒技术，不仅可以更加准确地判别程序行为，还可迅速恢复病毒对系统造成的破坏与修改，令您轻松摆脱病毒的困扰。
- 4、江民杀毒软件拥有强大的自我保护功能，能够有效避免病毒的肆意破坏和干扰运行，为自身和系统同时加上了“金钟罩”般的强力保护。
- 5、开启江民杀毒软件的网页数据流监控功能。该功能可以更好地防御各种形式的网页病毒，为您的网上冲浪撑起保护伞。
- 6、开启江民杀毒软件的 BootScan 功能，在系统登陆前进行病毒查杀，清除顽固病毒更加方便、彻底。
- 7、建议使用安全专家内置的 RootKit 扫描功能。该功能可以对恶意程序深度隐藏的项目进行检测和清除，使恶意程序无处藏身。
- 8、建议使用安全专家内置的漏洞扫描功能。该功能扫描系统漏洞更加全面、准确，修复速度更加快捷。同时新增常见第三方软件漏洞扫描功能，使防护更全面，保护更彻底，不给病毒利用漏洞进行传播的机会。
- 9、如果您尚未安装江民杀毒软件，推荐您使用江民免费在线查毒进行病毒查证。

利用小女孩及其母亲 僵尸网络钓鱼网银

来源：ZDNET 安全频道

国外媒体报道，近来出现一波源自墨西哥的新的网络钓鱼攻击。这个攻击利用了一则具争议性的新闻，新闻内容指称一名据称失踪的四岁小女孩 Paulette Gebara Farah 被发现死于自家的房间内。经过调查后，我们发现这波攻击来自一个墨西哥的僵尸网络/傀儡网络 Botnet，企图盗取使用者的银行往来相关资料。

拉丁美洲地区盛行使用线上金融交易，而这波攻击是网络犯罪份子以线上金融交易社区为目标，致力于侵占金钱与敏感财务资料的另一案例。

追踪该则新闻的使用者在进入网页便沦为攻击的猎物，网页内有一则相关 Paulette 的文章，并宣称会提供 Paulette 母亲的裸照。当使用者进入这个网页后，会看到一个假的对话跳窗，要求使用者下载及安装 Adobe Flash Player。



El día de ayer reportamos que la mamá de Paulette había sufrido fuertes amenazas y temía por la integridad de su familia. También dijimos que la mamá de Paulette está preocupada porque los ladrones (que asaltaron su casa la semana pasada) publiquen sus fotos personales en la red.

También les pasamos un video exclusivo en el que Juan Jos Origel, periodista de la OrejaTV declaraba tener las fotos de la mamá de Paulette que habían robado los ladrones y que en el momento en que las pida las entregará a la mamá de Paulette.

Sin embargo, hoy se supo que la periodista Martha Figueroa aseguró a una estación norteamericana que a ella también le han ofrecido las mencionadas fotos y que son muy comprometedoras pero no dijo en ningún momento que en ellas aparece desnuda.

Los periodistas de la OrejaTV dicen que la mamá de Paulette aparece en ligero, que son prendas femeninas interiores con elástico ([ver ejemplos aquí](#)). Se habla también que podrán existir fotos en topless en la playa con su novio. Sin embargo, la mamá de Paulette ha declarado a la Revista People en Español que sólo son fotos familiares.

Por lo que podemos concluir amigos que NO HAY fotos de la mamá de Paulette DESNUDA, como están diciendo algunos medios tremendistas. Y es más, si las hubieran tenían por descontado que NO APARECERÁN en la red, pues muchos medios mexicanos poderosos han puesto una especie de blindaje de protección a la diva adolescente.

Palabra del Blogdelatele!

图、假网站中的新闻内容屏幕画面

点击开始(Run)就会下载文件名为 video-de-la-mama-de-paulette.exe 的文件，这个文件实际上是傀儡僵尸网络的客户端程序，经 Trend Micro 侦测为 TSPY_MEXBANK.A。

在调查过程中，我们进入了僵尸网络的控制中心(command-and-control，简称 C&C)界面了解其管理功能。我们也进入了管理界面来亲眼目睹这个新傀儡僵尸网络完整的功能。

僵尸网络的目录显示出傀儡僵尸的总数及受入侵的电脑列表。傀儡僵尸的列表列出了客户的身份证号码及姓名，以及在僵尸网络中进行了那些活动。功能包括可开启或关闭傀儡僵尸，在傀儡僵尸上启动 netcat(可被用来当做后门使用，功能强大的网络工具)，以及从僵尸网络中移除傀儡僵尸等的选项。

新发现的僵尸网络的功能相当广泛，和其它较早出现，业已有相当发展规模的僵尸网络家族不

相上下。每一种功能都被安置在独自的模块中，让僵尸网络管理者可个别逐一地进行设定。

在僵尸网络所提供的功能中发现网址嫁接(pharming)模块也毫不令人感到意外。就如网络钓鱼模組的屏幕画面所示，这个特殊的僵尸网络目标为墨西哥的使用者，特别是当地 PayPal 的网站，及该国最大的银行 Bancomer。

除此之外，龙舌兰僵尸网络(Tequila botnet)也可从不同恶意 URL 中，透过 HTTP 或 FTP 来下载文件。这个新家族曾被发现投掷 ZBOT 的资料偷盗及假杀毒软件恶意软件。

不过一般消费者并非是这个僵尸网络幕后网络犯罪份子剥削的唯一对象，AdSense 模组会让网站与网站的广告重覆地被载入。事实上，网络犯罪份子利用此模组来提升网站的交通流量，增加广告网络如 Google 谷歌的 AdSense 所支付的费用。

除了被发现出现在恶意网站中外，龙舌兰僵尸网络(Tequila botnet)也可透过如 USB 装置及 MSN Messenger 等进入系统。僵尸网络会传送夹带了文件的讯息(以附加文档之类的方式)，或恶意软件的联结。

由于僵尸网络被破获，其数据中心服务主机的地点已不存在。但如果其开发者开始新的攻击并散布新文件，傀儡僵尸的数量将会再度增加，也会让开发者在未来再去为僵尸网络创作新的模组。

世界杯第一高危木马爆发 “呜呜祖拉”下载器感染 420 万电脑

来源：ZDNet 安全频道

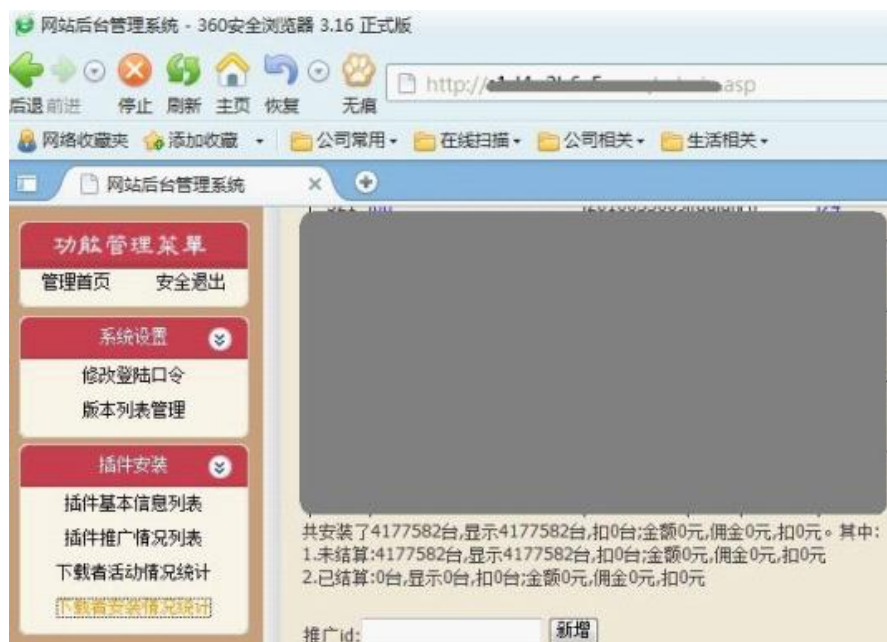
世界杯赛程刚刚过半，一个名为“呜呜祖拉”的木马下载器已迅速流行，并呈爆发之势。6月22日，360安全中心发布橙色安全警报称，“呜呜祖拉”木马已侵袭了大约420万台电脑，不但危害特别严重，而且也是目前最活跃的高危木马。

360安全专家石晓虹博士说，由于该木马在大量赌球、博彩网站上挂马，又与许多不良下载站提供的彩票软件捆绑传播，因此一跃成为世界杯期间最流行、对球迷上网危害最严重的木马。石晓虹提醒说，球迷在观看球赛直播时要忍受“呜呜祖拉”制造的噪音，上网看球、侃球，特别是研究彩票时更要提防“呜呜祖拉”木马的攻击。

据一些“呜呜祖拉”木马下载器的受害网友反馈：由于彩票分析和缩水工具大多是收费软件，他们搜索下载了所谓的“破解版”彩票软件，使用后才发现电脑中了招，不光桌面多出来大量广告图标，杀毒软件也无法打开。更严重的问题是，当这些网友想安装其他安全软件时，才发现根本无法装到电脑上，频频出现安装失败的情况。

360安全专家石晓虹博士介绍说，“呜呜祖拉”的典型特征就是屏蔽杀毒软件，再把数十个盗号木马和广告程序下载到中招电脑里，伺机盗取受害网民有价值的网上帐号。“很多彩民通过网银支付

来合买世界杯彩票，一旦中了‘呜呜祖拉’，网银密码就可能被木马通过记录键盘操作等方式窃取，直接造成经济损失。”



图片：“呜呜祖拉”木马下载器统计后台：共安装了 4177582 台电脑！

经 360 安全中心对木马样本的分析，工程师追踪到“呜呜祖拉”统计后台的数据惊人，木马安装量竟高达 4177582 台电脑，丝毫不亚于很多知名软件。“目前我们对‘呜呜祖拉’木马的传播途径仍未彻底了解，通过查看其后台，目前这个下载者似乎是一个代理商，其下面还有分销商，而此后台还应该有一上级的传播控制平台。因此，‘呜呜祖拉’木马的危害性可见一斑。”石晓虹说。

据悉，由于这部分中招网民电脑里的杀毒软件已被木马破坏，又难以通过其他软件实施救援，往往只能重装系统。为此，石晓虹博士建议广大网友，如果电脑桌面出现删不掉的快捷方式、杀毒软件无法使用等情况，应尽快下载使用“360 系统急救箱”，可以彻底清理“呜呜祖拉”木马。

据石晓虹透露，360 安全卫士用户电脑中的“呜呜祖拉”木马感染量极小，而且仅限于少量老版本用户。“这些用户只要将 360 安全卫士升级到 7.1 正式版及以上版本，其中的‘木马防火墙’能全面拦截各类木马攻击，使 360 不会被‘呜呜祖拉’等木马破坏，可以保护用户安全上网看球和买彩。”

“苍井空现象”诱发不良木马攻击剧增

来源：eNet 硅谷动力

在激情四射的世界杯之余，日本著名 AV 女优苍井空来华也引发了一股网络热潮。她开微博、做代言，几乎一夜间红透了中国的大江南北，媒体甚至将此惊呼为“苍井空现象”。然而在苍井空赚尽眼球的背后，却是不良网站木马攻击数量的大幅激增，据 360 安全卫士恶意网页监测数据显示：近一周来，360 日均拦截挂马网页数量超过 800 万次，比此前涨幅达到 30% 以上，其中色情不良网站成为木马最活跃的重灾区。

据了解，自上周高调出席上海某网游厂商代言活动后，苍井空在国内某搜索引擎风云榜一周热点榜单中高居榜首，搜索量达到 195618 次。“超高人气同时带来了高风险，以‘苍井空’为关键词的挂马网站每天都在新增几百个。”安全工程师说：“木马和不良网站长期狼狈为奸，如今很多网站打着‘苍井空’的招牌诱惑网民访问，如果不使用安全软件进行防护，一点开这些网页，电脑就会中招。”



图 拦截“博推网”苍井空相关挂马网页

附：6月21日被黑客挂马的部分苍井空相关网页信息：

【注意：为防止用户误点击，下列恶意网页的链接已做特殊处理。】

1、博推网

挂马网页：hxxp://www.myliuliang.org/news/58.html

2、免激网

挂马网页：hxxp://www.hk02.cn/Article/zuixin/2010-05-17/682.html

3、520 美女网

挂马网页: [hxxp://www.520de.com/html/ribenmeinv/20100514/3481.html](http://www.520de.com/html/ribenmeinv/20100514/3481.html)

4、美女人体艺术

挂马网页: [hxxp://www.xrtys.info/meinvrentiyishu/35_13.html](http://www.xrtys.info/meinvrentiyishu/35_13.html)

5、播友网

挂马网页: [hxxp://4x.q7.d.9534.info/article/](http://4x.q7.d.9534.info/article/)

产业动态

网游反盗号告别单打独斗 切断隐秘利益链条

来源：中国经营报

对网游行业产生了极大伤害的盗号问题已经到了不得不解决的时候。2010 年 6 月 15 日，一个“反盗号绿色联盟”的网游组织在试运行两年后于上海成立。该组织结合玩家、运营商、安全企业、交易平台、支付平台和公安或行业协会等产业界相关方，意在通过产业链合作、跨平台打击盗号销赃。

随着网游企业结束暴利增长时代，激烈的竞争态势下，很可能一个细节做不好，就会使游戏厂商丧失玩家和市场。如今市场上的网游产品越来越多，玩家一旦发生账号或虚拟物品被盗，常常因为无法追回或追回时间太久，而选择“离开”这款游戏。

要想让流失的老玩家“回心转意”，比吸引新玩家难度更大。更重要的是，盗号“顽疾”会破坏游戏的平衡性，影响运营商的口碑。盗号产业化规模越大，外界对于网游产业的质疑也越大。

告别“单打独斗”

由上海市信息服务行业协会发起成立的这个“反盗号绿色联盟”目前加入的成员包括盛大、九城等 30 余家游戏企业，据该协会数码互动娱乐专业委员会秘书长张明介绍，联盟与第三方交易服务商 5173、网络安全技术服务商中磐科技、反外挂安全技术服务商顶点唯峰、第三方支付服务商快钱等公司也建立了合作，后者与大型网络游戏直接对接。

“反盗号现象已经严重到了不得不管的地步，但这不是一个企业能够做好的，只有平台商和运营商达成协助性的共识，才能够使得保障玩家账号安全真正落实。”久游网副总裁兼营销总监吴军指出。

事实上，盗号是一个自网游出现之日，就已经存在的老问题。据不完全统计，我国现有网游用

户 6587 万人，其中付费用户 3715 万人，但超过三分之一用户因黑客等原因，蒙受账号、装备等虚拟财产损失。

在此之前，网游厂商、交易平台、支付平台等基本上都处于与“盗号者”单打独斗的局面。“网游厂商只能封锁可疑账号的使用、却无法为用户追溯损失的虚拟货币或虚拟物品，交易平台可截留虚拟道具的交易、但无法确定哪些交易物品是盗窃而来的，支付平台可将具体的交易金额返还、却不知道哪些交易背后是销赃行为。”

一位有账号被盗经历的玩家告诉记者，其经过诉求并提供严谨的证据，运营商已经可以很迅速地恢复自己的稀有装备了，但是梁华栋却被告知金币不能恢复。厂商的回答是为了确保游戏内不出现通货膨胀，但事实上，如果采取技术追踪手段，通过与网游道具的交易平台、支付平台公司合作，是可以将金币追讨回来的。

事实上，盗号也是一种犯罪，张明表示，但是目前这方面在司法上存在盲区。而账号或虚拟物品被盗，在伤害玩家利益的同时，也遭到各种质疑，导致整个产业链不安全。“不联合起来，任何一方都无法解决问题，尤其是在网游法规化进程日益紧迫的背景下，盗号、销赃涉及的金额已经越来越大，已经引起了各界的极大重视。我们结合玩家、运营商、安全企业、交易平台、支付平台和公安或行业协会等产业界相关方，形成产业链联动、各方共同协作保障用户账号安全，是‘反盗号绿色联盟’成立的初衷。”

盗号利益链条

如果说最初的盗号是案值不大的个人行为，现在的盗号已经越来越组织化和产业化。盗号难以“根治”，这背后是一个赚钱容易、回报丰厚的利益链条。

扬州市涉案金额最大的一起黑客案中，盗号者在法庭坦陈：“当黑客赚钱太容易了。”

一位资深游戏程序员告诉记者，“使用木马生成器，一个小学生就会做木马。木马可能很简单，但它窃取信息的后果却可能相当严重。”

上述游戏程序员表示，黑客案件的被发现率较低。由于计算机病毒的种类极多、更新速度又很快，所以黑客被警方发现的概率并不高。目前的黑客已经摆脱了散兵游勇的状态，以一种并不严密但却绝对保密的团体进行盈利活动。这个圈子一般是由两条线组成的，一条是专门负责技术也就是获取装备的，一条是负责销售通过前者获取的装备。

倒卖游戏装备的组织一般由总代理商和分代理的架构组成。中国创造的 260 亿网游市场使得他们不缺买家。利益驱使之下，往往可以在短时间内就获得巨额利益。以几个月前震惊一时的“温柔木马”案为例，该系列木马程序高达 28 款，盗窃游戏账号、密码超过 530 万组，涉及 16 个省市、涉案金额高达 3000 多万元。

资深业界人士、《电玩巴士》的主编梁华栋告诉记者，不同游戏的道具和账户，价值不同。以《魔兽世界》为例，其中的一个金币价值 2 分钱。一般的玩家会有 2 万金币，也就是 400 元。而工会的会长，会有十几二十万的金币，也就是价值两三千。这还不包括账号里各种各样的装备、道具。

“而《征途》游戏，本身很多物品都是玩家花重金购买的道具，如果一旦被盗，玩家损失几千甚至几万的，非常普遍。”梁华栋表示，盗号不仅让玩家付出时间、金钱的账号或物品被盗，更是影响了运营商的口碑。

“在竞争激烈、玩家选择多样的现在，一旦用户被盗号，可能会有长达三四个月的时间没法玩，如果无法追回自己的道具和金币，或者即使获得部分恢复，玩家可能也会丧失某些游戏里的能力，就意味着要重新玩起，这会导致玩家直接放弃该游戏。”梁华栋如是说。

对网游厂商而言，最难的是吸引新用户，新用户的吸引尚且如此之难，老用户如果因为非自身的原因流失，是更大的损失。因为老用户一旦流失，其有可能带来的新用户，包括绑定的用户群体会迅速瓦解和流失。

这正是目前的网游公司最担心的事情。

“为此，联盟的做法是，促使游戏营运商和虚拟物品交易平台合作开发了 API 自动交易系统追踪技术，以追踪盗号者的赃物和现金流向，并利用后台及时冻结和追回被盗赃物以及赃款。”张明说。

根据反盗号联盟的协作原则，第三方虚拟交易平台和第三方支付平台也将建立密切的沟通机制，利用相关交易信息和各种交易记录，全年配合游戏营运商和执法机构取证，为公安网监执法提供重要的线索，打击盗号、盗卡行为，为用户挽回损失。

网游交易平台 5173 相关负责人告诉记者，为了配合解决盗号纠纷，该公司有专门的反盗号小组，并设置一定时间的资金审核期，即使交易成功，也可以将物品追回，同时，玩家误买的被盗物品被游戏官方收回时，还可获得该平台的限时理赔。

张明指出，对于这些联盟成员而言，打击盗号本来就是他们的一项日常工作，因此目前在技术和成本的投入上仍然是以各自支出为主。

“我们正在与网游行业相关的政府部门协商，未来会得到更多的产业支持和资金支持。”张明透露，上海市经济信息委员会正在建立一个反盗号的专项资金，由于还在审核过程中，不方便透露具体数额，但是其足以对反盗号联盟的相关成员企业提供有力支持。

360 安全卫士争端

来源：国家财经周刊

不断增长的网络安全需求，让一款名为 360 安全卫士的软件，在功能上越滚越大。从“流氓软件”卸载，到修补系统漏洞；从木马、病毒查杀，到安全浏览器……高举免费服务大旗的 360 软件，市场版图快速扩张着。

对大多数的中国互联网用户来说，免费享受的网上安全服务，使他们暂时忽略了对软件安装的知情权和选择权。他们更加不会思考，当一款软件凭借免费策略而锁定数亿计算机用户时，原本正常的行业竞争逻辑是否会遭遇扭曲？

6月10日，金山、百度、搜狗、腾讯、傲游、可牛等10家公司针对近期互联网客户端软件行业“恶性竞争”、“无视用户选择权”等行为，联合发起“互联网软件自律联盟”。

在此之前的5月21日，金山公司称360安全卫士恶意卸载金山网盾。4天后，360安全卫士的开发公司——奇虎360(以下简称奇虎)董事长周鸿祎在微博上大爆金山公司的各种安全问题，金山安全CEO王欣随后在微博上回应，同时亦有数家公司加入论战。5月31日，奇虎与金山分别向对方发起诉讼，目前双方案件均已立案。

走出争议的漩涡还需要很长时间，而争议的起源则需要拨回4年之前。

出身公益

360安全卫士原本是一款“公益、中立的第三方软件”。

2006年7月，奇虎公司正式推出360安全卫士产品时，对这款互联网安全软件有着清楚的定位，即为用户提供免费的恶意软件查杀、系统诊断及修复、病毒查杀等功能，“净化互联网空间”。

当时的360安全卫士在奇虎公司内部只是一个不被关注的小项目。奇虎公司一份早期通讯录显示，360安全卫士整个团队只有不到10人。360这个名字也是项目负责人傅盛根据自己生日和身份证号码起的，带有很浓厚的个人色彩。

为体现其公益性质，奇虎公司甚至宣布，“将在适当的时机把360安全卫士的所有权转交到第三方机构。”

彼时正值“恶意软件”肆虐互联网，网友对强制安装和运行、干扰其他应用程序、自动弹出广告等种种恶意软件的“流氓”行径深恶痛绝。而传统杀毒厂商们对此并未推出很好的解决办法，因而360安全卫士在产品功能上对用户具有很强的吸引力。

安天实验室首席技术架构师肖新光认为，在360安全卫士问世之前，传统杀毒厂商在流氓软件这个问题上没有解决好。

“一些厂商认为流氓软件没技术含量，还有一些则担心法律诉讼和人情问题。”肖新光表示，“360很好地应用了‘二八定律’——与几十万种病毒相比，360面临的对手只有几百种流氓软件。”

“打击流氓软件让360一战成名。”一位前奇虎员工向《财经国家周刊》记者表示，“360在产品功能设计上非常贴近用户需求，通过口碑的力量迅速积累了大量用户。”

同时，奇虎在2006年8月承诺：360安全卫士作为一款公益软件，不以盈利为目的，并保证自己不变为恶意软件。同时成立了由知名博客、业内观察人士和媒体人士组成的督导委员会，监督360安全卫士履行承诺。

随后，360安全卫士又在漏洞补丁修复、软件管理、木马查杀等关键点上抓住了机会。“此前的杀毒体系都是在非互联网环境下的开发模式，但是有了互联网以后，病毒制造与传播成了一个完

整的产业链，因此 360 给杀毒领域带来了新的定义。”傅盛在一次活动上表示。

这一时间，根据艾瑞市场咨询的数据，360 安全卫士用户覆盖数从 2006 年 7 月的 272 万增长到 2007 年 6 月的 3157 万。2007 年 10 月，奇虎宣布 360 安全卫士用户量超过瑞星、金山，成为国内用户量最大的安全软件。

转身盈利

2008 年 8 月，5 名成员宣布退出 360 安全卫士督导委员会，称当初对督导委员会的所有承诺已经有所改变，委员会“事实上早已结束”。

督导委员会中的一位人士对《财经国家周刊》记者说，“360 开始是一个公益项目，后来走的免费路线则是一种独特的商业模式，不可能与商业化绝缘。”

奇虎随后发表声明，称“流氓软件产业链已基本消灭，360 安全卫士的主要任务转向查杀木马，感谢督导委员的工作。”同时，“奇虎 360 商业化有助于向用户提供更好的免费服务”，“欢迎督导委员会和 1.4 亿用户、2.3 亿网民共同监督。”

与此同时，奇虎的其他业务一直没有起色，反而是之前不被看好的 360 安全卫士成为最重要的业务。

2008 年 3 月，奇虎宣布 360 安全卫士正式从公司剥离出来，由奇虎股东共同出资 3.6 亿元成立新公司运作。4 个月后，奇虎正式发布采用 Bitdefender 引擎的 360 免费杀毒产品。至此，奇虎正式进军杀毒领域。

傅盛缺席了那次 360 杀毒产品的发布会。在后来接受媒体采访时，傅盛表示当时“已经开始休假”。8 月，傅盛正式从奇虎辞职。

傅盛的离开，亦被业内人士视为 360 安全卫士的重要转折点。在占据一定规模的用户装机量后，360 安全卫士更为主动地寻求免费背后的盈利模式。此时的 360 安全卫士已经拥有包括安全卫士、木马查杀、免费杀毒、软件管家、浏览器等在内的多个产品系列，可在“安全辅助软件”的定位上探索商业利益。

奇虎总裁齐向东在通过邮件回应《财经国家周刊》记者提问时说，360 安全卫士的主要收入来源包括代销 NOD32 杀毒软件、搜索分成、游戏联合运营、网址导航广告等。“将来与安全相关增值服务收入会快速增长，譬如安全备份存储、一对一人工电脑远程维修服务等。”齐向东说。

但一位不愿具名的业内观察人士认为，软件管家、联合运营等都不能作为支撑 360 安全卫士的终极商业模式。

颠覆者

在当初讨论是否推出免费杀毒时，奇虎公司内部曾经有过激烈的争论，除董事长周鸿祎外，管理层和董事会的其他人都表示坚决反对。一个重要原因是当时 360 安全卫士在代销收费杀毒软件上收获颇丰。

“已经达到一年有几亿元。”齐向东说，“这一收入的成长性毋庸置疑，推出免费杀毒会使这

一收入来源基本归零。”

最终周鸿祎力排众议，认定免费杀毒是大势所趋。

免费模式极大拓展了 360 安全卫士的市场份额。按奇虎的官方口径，360 安全卫士目前已拥有 3 亿用户；360 杀毒的月覆盖人数比例达 50%，拥有 2 亿用户。

一位安全软件领域资深人士表示，“360 一路走来，恶意软件查杀、漏洞补丁修复和软件管家前三步精彩绝伦，非常符合用户体验和互联网原则。但在免费杀毒上，360 并没有合理描绘出收入模型，破坏了整个产业的价值链基础。”

“在中国通用软件领域里，桌面反病毒是最大的一块蛋糕。”该资深人士说，“360 通过打击一个年销售额 10 亿元的反病毒产业，造就了一家年营业额不足 2 亿元的公司。但由于产出能力低，只能通过破坏式的竞争维持生产力，不惜毁灭产业为代价。”

对此，齐向东反驳说，杀毒行业规模在最近 10 年仅增长一倍左右，远低于互联网和 IT 行业的增长率，这是极其不健康的。“我们预计未来五年，互联网将把杀毒行业的收入规模扩大 10 倍，即从 10 亿元增长到 100 亿元。”

前述 360 安全卫士督导委员认为，传统杀毒软件公司过于软件化，必然被互联网公司冲击，互联网的特点就是开放与用户体验。“但免费不是互联网的本质特征，在安全这个特殊市场里，我更赞同付费模式。”他说，“其实免费和付费不是最核心的问题，关键是要用市场化手段合理合法地去做事情。”

“互联网是产品下载通道、用户付费通道、销售通路、推广渠道，我们是通过互联网来做安全，解决互联网上的问题。”金山安全 CEO 王欣对《财经国家周刊》记者表示，“而某些公司是通过安全来做互联网，以安全的名义做浏览器、下载站等。商业模式还是不一样。但商业竞争必须遵守行业规则，首先尊重用户选择权利。”

可牛是一家刚刚进入的免费杀毒软件公司，该公司 CEO 正是从前出走于奇虎的傅盛。他在谈到互联网对传统杀毒软件行业冲击时表示，“免费模式无可厚非，但免费的另一含义是自由，不能因为提供免费服务就控制用户。”

安全还是控制？

傅盛所说的“控制用户”，是指可牛杀毒被 360 安全卫士拦截的事件。

5 月 25 日，可牛杀毒软件发布还不到 5 分钟，就有网友反馈，下载后打开可牛杀毒安装文件即遭到 360 安全卫士的拦截。提示框显示“正在安装的软件会破坏 360 为您提供的安全防护”，同时只有一个“停止该软件安装”的默认选项和“确定”按钮。

可牛对 360 安全卫士 5 月 23 日和 5 月 24 日的升级包进行分析，发现“360 赶在可牛杀毒发布前，就制作好了拦截数据库，以方便在可牛杀毒发布后，第一时间就开始拦截。”

分析还发现，拦截指令是由 360 安全卫士的云服务器来发出。因为都是云端控制，“这样就很难取证。”傅盛说。

“反病毒软件从来都在相互卸载，因为会在系统底层发生冲突。”上述安全领域资深人士针对此事说，“后装的能卸载已经安装的，这个机制是合理的，用户有选择权和后悔权，这次的拦截把‘后卸前’的约定规则打破了。”

“360 没有拦截可牛杀毒软件。”齐向东说，“我们注意到网上的消息，对于可牛方面提供的截图，我们不清楚是从哪里来的。只有经过公证的页面才是可信的。”

如果说 360 安全卫士拦截可牛还给出选择的话，对傲游浏览器的拦截，则是直接将其认定为“危险木马”，用户只能选择“立即清除”或“暂不处理”。

傲游 CEO 陈明杰说，傲游从前是 360 软件管家里的推荐软件，但在奇虎推出自己的浏览器产品后，傲游浏览器就变成了 360 安全卫士的拦截目标。

此外，一款名为“恶意软件清理助手 2010”的软件也遇到了类似的问题。该软件制作负责人对《财经国家周刊》记者表示，“我们从 2004 年就开始开发清理助手，目前每天的在线用户量约为 10 万人。最近突然被 360 安全卫士报告‘正在攻击 360 安全卫士’，还给出了‘恶意软件清理助手会导致安全保护失效，并对电脑和个人资料造成危险’的提示。”

中国互联网络信息中心(CNNIC)和国家互联网应急中心联合发布的《2009 年中国网民网络信息安全状况调查报告》显示，有近一半(49.3%)的网民无法清楚区分杀毒软件、木马查杀和清除流氓插件等安全软件的功能和用途。

上述安全领域资深人士表示：“现在很多厂商站出来，背后并非是免费和收费之争的问题。以前软件行业约定俗成地保持互相兼容，都在一个平台上才能给用户选择。不能因为你的用户量大，口碑好，就根据某些软件的某些缺点作为屏蔽它的理由。应该是由用户来决定，而不是某一个软件来决定。这才是核心问题。”

对于这种说法，奇虎总裁齐向东表示，作为安全厂商，360 安全卫士有义务向用户告知其电脑中到底发生了什么，并由用户选择将做什么操作以符合用户自己的利益。“这是 360 认为自己所应该负有的责任。”

世界杯火爆 Twitter 宕机 SNS 需要投怀云计算？

来源：孙永杰

近日，由于南非世界杯及某些功能的上线，全球最大的微博平台 Twitter 的服务数次中断。据统计，在今年 6 月之前的半年里，Twitter 宕机时间总长为大约 9 小时，而在过去一周 Twitter 宕机时间已经超过 5 个小时，尤其是从 6 月 8 日到 6 月 16 日的 9 天时间里，Twitter 网站仅有一天完全正常，其中有四天的宕机时间达到一小时左右。对此，Twitter 负责公关事务的西恩·加雷特(Sean Garrett)

近日通过官方博客解释了近期 Twitter 多次宕机的原因。即世界杯赛期间流量突然激增及 Twitter 的应对措施又不够得力。尽管 Twitter 方面声称会不断改进平台的性能，但在网络流量高峰和升级的时候，代表 Twitter 故障的那条鲸鱼还是可能会出现在网页上。也就是还是会出现宕机。

笔者认为，近期 Twitter 频繁的宕机，一方面说明 SNS 对于用户的重要性及未来增长的前景，这本来是令以 Twitter、Facebook 等为代表的 SNS 们感到高兴的，但另一方面如果在未来的发展中，SNS 不能采取有效措施来减少，甚至杜绝类 Twitter 频繁宕机现象出现的话，不但会影响到 SNS 间的竞争格局，还可能会为 SNS 的发展(尤其是商业化)蒙上阴影。

例如最近一连串的 Twitter 宕机事件，业内就已经开始质疑这家风靡全球的微博平台能否应对不断增加的流量。其实业内的质疑还在其次，主要是用户。因为用户除了平时使用 Twitter，在遇有重大或突发事件时，更会希望利用 Twitter 来了解和分享彼此的信息和感受(例如本次的南非世界杯)，这也是导致负载陡增的原因，这时候如果不能满足用户的需求，Twitter 受到的负面影响可能比平时要大得多，但 Twitter 几乎是在这种情况下出现宕机。如果这种状况不能很好解决的话，原有的用户很可能在未来转向其他的 SNS，例如 Facebook(据称 Facebook 在南非世界杯期间，至少到目前为止没有出现像 Twitter 一样的宕机现象)，或者间接影响到未来新的用户来使用自己的 SNS 平台及服务。笔者在此的意思是说，频繁的宕机一方面会让用户对于 Twitter 本身产生质疑，进而转向自己的竞争对手，还会影响到对于 SNS 的参与度。这无论是对于 Twitter，还是 SNS 的发展都是不利的。

其次就是 Twitter 也好，Facebook 也罢，在目前用户和规模发展势头迅猛的形势下，都开始谋求商业化发展之路。从商业模式上看，Twitter 正计划通过 Promoted Tweets 广告服务增加公司营收，而 Facebook 除了传统的互联网广告(例如显示广告)外，也期待通过 Facebook Credit 增加营收途径。从广告的角度看，事件驱动的广告是客户最为看重，也是效果最为明显的，同时对于 Twitter 或 Facebook 也应该是开价最高的，可如果在这个时候频频出现宕机，不但会给客户造成损失，广告达不到预期的效果，更关键的是，让客户怀疑 SNS 商业化的能力，直接影响到 SNS 的商业化进程和营收是最致命的。除了广告(面向客户)外，像面向用户的 Facebook Credit 更不希望频频遇到宕机，原因很简单，因为用户毕竟是付了钱的。如果在用户付费的情况下，当他们在某些特殊事件下最为需要 SNS 服务的时候，怎么能够容忍宕机呢？

那么 SNS 面对随时变化的用户需求如何才能最大限度降低宕机出现的频率？

其实在近期 Twitter 频频宕机之时，另一家全球最大的 SNS 社交游戏平台 Zynga 则已经通过当今最新的云计算为其他 SNS(例如 Twitter 的宕机)提供了很好的借鉴。提到 Zynga，人们马上就会想到其去年 6 月发布的《开心农场》(Farmville)游戏。其实在该游戏发布之初，Zynga 对于用户数的预测并不高，这使得随着用户数飞速的增加，Zynga 自己支持该游戏的服务器从几十台增长至好几千台，但仍不能满足用户增长速度的需求。所以 Zynga 借助了亚马逊 EC2(Amazon Elastic Compute Cloud)云存储服务，保证了游戏的运营。对此，Zynga 网络运营副总裁马克·威廉姆斯深有感触地认为，这一决策非常幸运，考虑到这款游戏巨大的增长速度，没有亚马逊相助的话，《开心农场》早已失败。

而自此之后, Zynga 改变了游戏发布模式。即 Zynga 的每款游戏都首先在 EC2 平台上发布, 并持续观察三到六个月, 如果游戏增长乏力或是前景可预期, Zynga 就会把游戏从亚马逊 EC2 迁回自己的数据中心; 如果游戏增长迅速, Zynga 就让其分别运营于亚马逊 EC2 和 Zynga 数据中心的的游戏比例保持在一半对一半, 或 3、7 开(也有可能是 7、3 开)。笔者认为, 对于 SNS 自身(用户请求或突然增加, 或减少, 或稳定)的特点来说, Zynga 这种借助云计算(不把鸡蛋放在一个篮子里)的做法颇值得借鉴, 因为云计算满足了 SNS 对于稳定性, 可伸缩性及不间断性的要求, 而且可以节约成本(这对于尚在赢利中的 SNS 也不容忽视), 降低了单独自身运营的风险。试想一下, 如果之前 Twitter 像 Zynga 一样借助云计算的话, 近期的宕机事件是否可以避免或者减少呢?

通过上述 Twitter 近期的频繁宕机以及 Zynga 借力亚马逊云计算的成功, 笔者认为, 作为当前互联网和 IT 产业最为业内看好的 SNS 和云计算似乎有着天生的联姻基因, 也许未来 SNS 的发展将会更多拥抱云计算, 而云计算也为自己找到了新的用武之地。

谷歌收购 AdMob 细节:5.3 亿股票加 2.2 亿美元现金

来源: 新浪科技

据国外媒体报道, 谷歌周五提交给美国证券交易委员会(以下简称“SEC”)的文件显示, 该公司对移动广告公司 AdMob 的收购动用了 5.3 亿美元股票和 2.2 亿美元现金。

在此之前, 谷歌只对外宣布, 这起收购的总值为 7.5 亿美元, 但并未透露具体财务构成。而该公司提交给 SEC 的文件显示, 其中包含了 5.3 亿美元股票以及 2.2 亿美元现金。

谷歌经常会利用股票作为收购资金, 通过这种方式来减少对现金的使用。该公司目前的现金储备约为 265 亿美元。

谷歌对 AdMob 的收购曾经遭到美国联邦贸易委员会(以下简称“FTC”)的反垄断调查。在该收购计划宣布半年后, 谷歌于今年 5 月底完成了对 AdMob 的收购。此前一周, 该交易刚刚获得 FTC 的批准。

杭州首例非法获取公民个人信息案一审宣判

来源：新华网

杭州首例非法获取公民个人信息案 17 日在拱墅区人民法院开庭。被告人崔正东被判处有期徒刑一年，罚金 5 万元。

检察机关指控，2008 年 9 月至 2009 年 10 月期间，被告人崔正东通过互联网购买、交换等非法手段获取大量如车主信息、股民信息、房产业主信息、手机信息等公民个人信息，并通过互联网将信息出售给他人。2009 年 9 月初，黄梅花、黄摇进等人从被告人崔正东处购买了车主信息，通过恐吓短信敲诈他人(两人均已被判刑)。其非法获取公民个人信息，情节严重，已触犯刑法第 253 条之规定，犯罪事实清楚，证据确实充分，应以非法获取公民个人信息罪追究其刑事责任。

法庭经审理后作出一审判决，判处被告人崔正东有期徒刑一年，罚金 5 万元。崔正东表示服从宣判。

思科升级云安全平台 推电子邮件与 Web 安全服务

来源：比特网

许多企业都需要基于云的协作和通信解决方案，为移动员工队伍提供随时随地使用任何设备访问关键数据的能力。很自然，这种规模的协作和通信存在着越来越高的安全风险，因为许多网络访问是在传统的企业防火墙之外进行的。为了解决这些问题，思科推出了永远开启、基于云的 Cisco IronProt™ Email Data Loss Prevention and Encryption(电子邮件数据丢失防御与加密)，以及 Cisco ScanSafe Web Intelligence Reporting (思科 ScanSafe Web 智能报告)服务。这些服务提高了企业安全解决方案的灵活性，降低了管理需求，稳定了成本，并通过提高网络的可视性使企业能够更好地控制网络，同时还能够使企业保持法规遵从。

思科最新对云安全产品进行的创新包括：

- Cisco ScanSafe Web Intelligence Reporting(思科 ScanSafe Web 智能报告)——WIRe 是 ScanSafe 公司开发的业务智能平台，该公司于 2009 年 12 月被思科收购。WIRe 使企业能够了解其 Web 资源的使用情况，以确保关键业务应用不会受到与业务无关的数据流影响为中心。只需几秒钟，WIRe 就可以提供详细的用户级信息，并对 Web 的通信活动提供广泛的信息。WIRe 提供了 80 多种预先定义的报告，能够根据 87 种不同的特性对活动进行报告和过滤，其中包括搜索条件和员工带宽随时间变化的使用情况。通过清楚地了解进入网络和网络中存在的数据流类型，企业可以拥有高度的自信，相信自己的企业信息是极为安全的，并且所有的恶意软件和不适当的内容都被拦截在外。

- Cloud-based Cisco IronPort Email Data Loss Prevention(基于云的 Cisco IronPort 电子邮件数据丢失防御)——思科的云电子邮件数据丢失防御解决方案利用了 Cisco Cloud Security Services(思科云安全服务)的强大功能，是全面、准确且简单易用的解决方案，有助于对于从云向外发送的电子邮件进行保护，并且可帮助客户满足法规的要求。这一数据丢失防御解决方案，是为需要为敏感数据提供高水平的保护，但又不想自己管理基础架构的企业所设计。此外，该服务还为客户提供了托管的电子邮箱以及法规遵从和可接受使用策略等优势。该解决方案提供了与全球协调、法规遵从、地区性法律、知识产权保护以及可接受使用等有关的 100 多个预定义策略。强大的深层扫描引擎对 150 个参数进行检查，在文件中对文件进行扫描，并对相似的关键字进行分析，这些功能将误报率降低至不到百万分之一。我们还提供了集成加密作为补充选项，进一步增强了这一独特产品的优势和价值。

思科对云安全的投资

为了支持其安全无边界网络架构，思科公司构建了强大的云安全部署。思科运营着 30 多个全球数据中心，为 100 个国家的客户提供极致的可靠性。事实上，思科客户已经连续 7 年享受了接近 100% 的正常运行时间。思科的云安全解决方案每天处理着大量的活动，包括 28 亿次名誉查询、25 亿次 Web 请求以及对超过 2500 亿封垃圾邮件进行检测。Cisco IronPort 防垃圾邮件解决方案被全球范围的机构所采用，保护的设备超过 2.35 亿台。这些解决方案由自动化智能系统和思科 100 名专职工程师提供支持，以确保思科的云安全能够有效地保护客户的网络。

赛门铁克发布最新月度安全报告

来源：新浪科技

近日，国际知名安全软件厂商赛门铁克发布了最新的《全球垃圾邮件及钓鱼网站月度统计报告》(State of Spam&Phishing A Monthly Report)。报告显示，2010 年 4 月份全球垃圾邮件继续在高位徘徊，而应用 CN 域名的垃圾邮件已经从 3 月的 4.1%降至 2.2%，降幅将近 50%，CN 域名的安全应用环境得到了再一次提升。

统计报告显示，2010 年 4 月份垃圾邮件在全球电子邮件流量中的比重高达 89.22%，与三月份的 89.34%基本持平；在垃圾邮件起源地方面，美国继续以 24%的比例位居第一位，印度、荷兰、巴西、德国分列第二到第五位，而网络钓鱼起源地方面，美国仍然以超过半数的比例位居第一位，而这主要是因为 52%的网络钓鱼网站的主机位于美国，比三月份增加 1 个百分点；另外以 6 月份世界杯为主题的恶意攻击也有增加趋势，例如黑客扮成世界杯赛事其中一家赞助商，并以葡萄牙文写成一个伪造邮件向用户发放，再采用中国澳门 IP 以掩人耳目。

报告还对垃圾邮件的域名应用比例进行了分析，数据显示，COM、RU、ORG 等域名成为垃圾邮

件的前三大"受害者",其中应用 COM 域名的垃圾邮件比例从 3 月的 47%飙升至 4 月的 62.7%,增幅高达 15%;俄罗斯国家域名.RU 自 4 月 1 日实施实名注册后,垃圾邮件比例虽然高达 22.1%,但相对于上月的 29.8%来说下降明显;ORG 域名紧随其后,相对来说所占比例不高,但也达到了 6%;而我国的 CN 国家域名则从 3 月的 4.1%降至 2.2%,降幅将近 50%。

报告显示,近一个月来全球钓鱼邮件比例有所上升,平均每 237.1 封电子邮件中就有 1 封钓鱼邮件,和 4 月份相比增长了 0.2 个百分点,英国再次成为钓鱼邮件攻击率最高的国家。来自中国反钓鱼网站联盟发布的月报也显示,2010 年 4 月该联盟受理并暂停域名解析的钓鱼网站为 1785 个,较上月增长 70%,约 4500 万网民因"网络钓鱼"蒙受损失。其中 COM 等域名下的钓鱼网站总数为 1689 个,占本月被处理钓鱼网站的 95%。

此外赛门铁克还指出,隐藏恶意软件的新网站成为增长最快的网络威胁,1,770 个新网站存在恶意软件、广告软件等潜在威胁程序,较 4 月份这一数字增长了 5.6 个百分点。对此中国反钓鱼网站联盟专家表示,网民应养成查看网站资质信息的习惯,借助第三方权威认证的企业登记信息、网站域名注册信息等资质来判断网站真实身份,从而规避网上交易风险。

记者了解到,今年以来中国源发垃圾邮件数量呈明显下降趋势,已经成功摘掉了垃圾邮件大国的帽子,而此前数年中国都排在全球垃圾邮件大国的前五位,2006 年甚至排名全球第二位。分析人士指出,从去年年底开始的 CN 域名治理行动是我国垃圾邮件大幅下降的决定性因素,有效遏制了 CN 域名下的不良应用,钓鱼网站等不良网络应用因此失去了在 CN 域名下生存的空间。

360 微博回应搜狗浏览器网速保护被报木马

来源:新浪科技

新浪科技讯 6 月 23 日晚间消息,搜狗 CEO 王小川微博中称搜狗浏览器“网速保护”内测专版被 360 安全卫士报为木马,对此,360 安全卫士微博回应称 360 用搜狗的公开版本验证后并未重现。在搜狗论坛上及用搜索引擎进行全网搜索,暂时也没找到类似的用户反馈。

360 安全卫士表示“有一种可能是王小川先生用的内测版未打上数字签名,或进行了一些敏感操作,导致 360 木马防火墙误报。希望搜狗方面能提供所反映的浏览器内测版本,以便进一步验证。”

360 安全卫士还称“经常有软件声称遭到 360 拦截,其中有的是误报,有的是软件本身有问题,还有的截图干脆就是伪造的。如果是误报,请及时与 360 联系,我们会尽快解除。有些竞争厂商声称遭到 360 恶意拦截,但既不沟通,也不提供样本的,我们也没办法。希望他们能去公证处公证,拿有法律效力的证据说话,而不是借机炒作上位。”

两成 Andriod 应用程序存在安全威胁

来源：ZDnet

在 Andriod 的应用软件商店的 48000 个应用软件中，大约有 20%允许第三方应用程序访问敏感的个人数据。

安全公司 SMobile Systems 在它们的 Andriod 市场威胁报告中表示，有一些应用程序被发现可以做一些事情，比如没有经过手机主人的允许自动拨打电话或者发送短信。例如，5%的应用程序会拨打电话给任意号码，2%的应用程序会通过程序自身发送未知短信给特定的号码，从而导致巨额通信费的产生。

SMobile Systems 的首席技术官 Dan Hoffman 表示，同时，有数十种应用程序被发现采用一些类似我们常见的间谍软件的手段，来获取敏感数据，包括获取电子邮件、文本短信、手机通信记录以及手机所处位置的信息。

他认为，“不要因为它们来自于一个知名的地方，比如 Andriod 软件商店或者为 iPhone 准备的 Apple 软件商店，所以我们就觉得它们似乎应该没有恶意代码或者在软件商店中有完善的审查程序。”

用户想要从 SMobile Systems 或者其他网站下载一个合法的，没有恶意代码的软件，但是他们永远没有一个好的办法来表明软件的作者是否有着良好的信誉，因为软件作者一般都使用网名，或者在软件中没有一个可以链接到官方网站的链接。

Hoffman 表示，“要知道，市面上已经存在有间谍软件，并且这个问题越来越严重。”

技术前沿

云安全联盟（CSA）公布云安全七宗罪

来源：网界网

惠普和云安全联盟近日列举出云安全七宗罪，如果你要将自己的应用迁入云中，那么最好提前认识清楚这些“罪状”。看看你或你的云服务商是否犯下了这些罪状？

数据丢失/泄露：到目前为止还没有一种被广泛认可的安全级别，能够控制云中的数据安全。有些应用之所以会泄露数据是因为脆弱的 API 接入控制，以及密钥的生成、存储和管理不善。而且好的数据销毁策略也不存在。

共享技术漏洞：在云中，一个不正确的配置参数可能会跨整个网络环境到处复制，也就是说，会有众多的虚拟机共享同一配置参数。可考虑的解决的办法是，为补丁管理强制执行服务等级协议(SLA)，为网络和服务器配置实施最佳实践。

心怀恶意的内部人：云服务商对其人员执行的背景审查级别可能会因企业对于控制数据中心访问的需求不同而不同。很多云服务商所提供的服务很好，但是和委托企业之间却存在着严重的信息不对称。应考虑执行服务商评价，规划好服务商员工的审查级别。

账户、服务及流量劫持：企业有大量的数据、应用和资源集中在云中，而如果云服务商的认证存在漏洞，那么入侵者便可轻松进入客户的账户，进而控制客户的虚拟机。建议对危险进行事前监控和双因素安全认证。

不安全的编程接口(API)：把云视为一个新的平台，而不仅仅是一个将应用开发外包出去的所在，这是很重要的。应在应用的整个生命周期内执行数据核查程序，开发人员应了解并执行某些与安全认证、接入控制和加密相关的规则指南。

云计算的滥用和恶意使用：坏人会比好人更具侵略性地使用云计算技术。我们看到，有很多黑客在将新的威胁手段和云计算的迅速结合方面颇为擅长，可以轻松地扩张或收缩威胁的规模。而一切仅需一张信用卡便可打开大规模威胁的闸门。

未知的风险：透明度的问题将会继续困扰着云服务商。有账号的用户只是和前端的界面互动，事实上并不知道后端有什么。谁知道服务商使用的是什么平台，什么级别的补丁？

从 C.I.A 三性看云计算的数据安全

来源：中国信息安全博士网

云计算概述

本文档的目的是对云计算中的数据安全进行浅析。因此在进行文档详述前，先对文中即将使用的云计算中的几个概念进行阐述。

1. 公共云

由某个组织拥有，其云基础设施对公众或某个很大的业界群组提供云服务。

2. 私有云

云基础设施特定为某个组织运行服务。可以是该组织或某个第三方负责管理，可以是场内服务(on-premises)，也可以是场外服务(off-premises)。

3. PaaS

即云平台作为服务。

提供给用户的能力是在云基础设施之上部署用户创建或采购的应用，这些应用使用服务商支持的编程语言或工具开发，用户并不管理或控制底层的云基础设施，包括网络、服务器、操作系统、或存储等，但是可以控制部署的应用，以及应用主机的某个环境配置。

4.SaaS

即云软件作为服务。

提供给用户的能力是使用服务商运行在云基础设施之上的应用。用户使用各种客户端设备通过“瘦”客户界面（例如浏览器）等来访问应用（例如基于浏览器的邮件）。用户并不管理或控制底层的云基础设施，例如网络、服务器、操作系统、存储、甚至其中单个的应用能力，除非是某些有限用户的特殊应用配置项。

5.IaaS

即云基础设施作为服务。

提供给用户的能力是云供应了处理、存储、网络，以及其它基础性的计算资源，以供用户部署或运行自己任意的软件，包括操作系统或应用。用户并不管理或控制底层的云基础设施，但是拥有对操作系统、存储和部署的应用的控制，以及一些网络组件的有限控制（例如主机防火墙等）。

传统数据安全

1.传统数据分类

一般情况下，我们依据“动”和“静”将数据分为存储的数据和传输中的数据。

所谓“静”即数据在存储，为了保护数据的安全，可以将数据依据安全需求的等级进行不同的存储保护；

所谓“动”即数据在传输的过程中，此时需要关注的不仅是需要保护的数据，还有数据流通的传输链路。

2.数据的安全

对于存储中的数据，需要依据数据的重要性和机密性级别，设计数据存储的方式，并且针对数据级别设计数据的备份及恢复策略，当然，还会对数据存储的数据库和服务器进行良好的访问控制，对服务器存储机房进行物理访问控制，这样才能真正保护存储数据的安全。

对于传输中的数据，我们会依据数据的重要性不同，进行不同级别的保护。如传输用户名密码等重要信息时，会采用加密的技术，而在采用加密技术时，也会依据不同的需求采取不同的加密措施；在路由信息等都需要进行保护时，会采用链路加密技术，在只需要保护净荷值时，可以采用端到端加密技术等；在传输大量采集信息时，可能会设计编码格式，使传输高效且安全。

云计算中的数据安全

无论使用 IaaS、PaaS 还是 SaaS 这三种模型中的任何一种，数据安全都较以往而言更为重要。

因此，我们需要对云中的数据安全进行浅析；虽然云计算是新兴的事物，但是对于其中的数据安全，我们可以试着用传统的 C.I.A（即：Confidentiality 机密性、Integrity 完整性及 Availability 可用

性)三性进行剖析,来看看云计算中的数据安全。

1.传输数据

对于传输数据,在使用公共云时,无论使用 IaaS、PaaS 还是 SaaS,都需要考虑对数据的传输是不是已经部署了恰当的加密方式。

对于传输数据,首先需要确保的是机密性,即使用一定的加密程序,比如 vanilla,或直接使用 FTP 协议和 HTTP 协议等情况;当然,对传输数据,尤其在互联网上传输数据,要确保的不只是机密性,还需要考虑完整性,比如是否使用 SSL 上的 FTP 协议(即 FTPS);是否使用 HTTPS 协议;是否使用安全拷贝程序(SCP)等。

2.存储数据

依照以往的思维,我们会认为对于存储数据进行加密是很必要的,但是其实在云中,事实并非如此。

如果你使用 IaaS 云服务做一些简单存储的服务,那么无论使用的是公共云还是私有云都可以进行加密;但是如果使用 PaaS 或者 SaaS,使用其基于云的应用,那么加密就不一定可行,因为加密会导致索引和检索的不便,导致上层部署机制的不可行,影响可用性,因此,此时存储的数据并不应该加密。

一般来说,使用基于云的应用存储数据时会将数据与其他数据进行混合,比如 Google BigTable(下文会稍作介绍),而且应用也会设计一些安全特征,比如数据标签等来防止未授权的访问,但是通过攻击应用的弱点等方法仍然可以达到未授权访问。

另外,在云中进行的数据处理过程,数据也是同样不能加密的。

3.数据举例

前文提到的 Google BigTable: 分布式结构化数据表

BigTable 是 Google 开发的基于 GFS 和 Chubby 的分布式存储系统,Google 的很多数据,包括 Web 索引、卫星图像数据等在内的海量结构化和半结构化的数据,都是存储在 BigTable 中的。

BigTable 是一个分布式多维映射表,表中数据通过一个行关键字(Row Key)、一个列关键字(Column Key)一级一个时间戳(Time Stamp)进行索引的。BigTable 的存储逻辑可以表示为:

```
(row:string, column:string, time:int64) -> string
```

很明显,对于 BigTable 进行索引时不能使用因为数据加密等原因而造成索引的失效。

4.数据加密新技术

由于云中存储数据为海量数据,因此加密过程会一定程度上影响处理的效率,对此各不同的云服务提供商均依据自己的情况部署了不同的控制措施,比如,分析加密点部署的位置,是在终端原点还是在存储服务器,另外,还需要考虑使用加密算法的速度是否能赶上磁盘 I/O 的速度等等。

由于加密和解密数据或文件十分消耗资源,因此现在有新的技术应蕴而生。

比如数据着色(data coloring)技术和云水印(cloud watermarking),都是针对云计算而发明的

数据加密技术。通过对数据进行不同的着色，对云打上水印，从而达到数据加密的效果，而又不会很耗费资源。

5.C.I.A 分析

从传输数据和存储数据的方向分析了数据的机密性、可用性和完整性后，现在直接对 C.I.A 三性进行下分析。

Confidentiality 机密性

在公共云中，机密性需要从两方面进行考虑。

一是通过认证和授权的访问控制来保护数据；但是对于云来说，控制的粒度较粗，而且一般云服务提供商也会使用较弱的认证机制。对于访问控制的问题将在后续的学习中详细描述，本文略。

二是存储的数据如何真正的进行保存，当然包括数据如何加密。用户可能希望知道，他们的数据在云中是怎么加密的呢？用的什么加密算法？密钥有多长？其实这些不是他们能够决定的，主要还是取决于云服务提供商。比如，EMC 的 MozyEnterprise 使用加密技术加密用户数据，但是 AWS 的 S3 却并不对任何用户数据进行加密。

在选择加密措施时，必须考虑云服务提供商能够提供的加密算法、能够提供使用的密钥长度，还有其对于密钥的管理机制。

Integrity 完整性

刚刚我们讨论了云中数据的机密性保护，现在看看完整性如何保护。

首先，进行数据完整性的保护不能依赖加密算法了，而是使用加密认证码（MAC），最简单的方法是对已加密的数据使用 MAC 值进行完整性校验。

另外，数据完整性的重要点，尤其是在大容量存储的 IaaS 中，是一旦用户拥有几个 G 甚至更多的数据在云中存储时，用户如何检查数据完整性？IaaS 传输开销是与移动的数据相关的，一个用户如果想验证其存储在云中的数据完整性，如何不需要下载数据？这是云中数据安全的一个要点，由于云中的数据是动态的且经常改变，因此也就是传统的完整性检查技术无计可施。

目前，业界已经开始提出对大容量数据的完整性校验提出了对动态存储数据校验的新的思路。

Availability 可用性

机密性和完整性讨论过后，我们来看看数据可用性。

首先用户要明确自己选择的云服务提供商能够提供什么样的服务，寻找真正适合自己的服务。

当然数据的可用性肯定会受到来自互联网络的攻击，需要云服务提供商进行一定的安全部署。

最后也是最重要的，真正的可用性其实是由云服务提供商的自身能力决定的，比如 2008 年 7 月，Amazon 的 S3 遭受了长达 8 小时的资源耗尽导致的服务停止；2009 年 2 月，Coghead 公司突然倒闭，只给用户 90 天时间来将数据迁移出。

因此可用性的考虑，最重要的是对云服务提供商的考虑。

结束语

其实，无论是机密性、完整性还是可用性，都需要由云服务提供商进行保障，通过其服务水平协议（SLA）进行提供给用户。

当前，云还并不是一个成熟领域，但是对于数据安全的考虑却需要在云建立之前进行把控，以避免给用户带来的损失。

IT 发展趋势驱动全新安全方法

来源：计世网

当今时代，私人邮件、照片、音乐日益增多，企业与政府部门的金融系统及客户记录也变得日益复杂，这些均表明信息无时无刻不在飞速增长，而同时管理信息也就变得日益艰难了。当然，信息已经不仅存在于你桌上的文件夹里，而是在你的手机、电脑或者上网本里。因为，人们希望无论是在办公室里、在家里或是在路上，都能随时随地接触到这些信息。

2010 年将是发生巨大变化的一年，是步入下一个十年的开端。在这一年里，我们需要更密切地关注信息，即它从哪里来、我们能对它做些什么、如何管理它，以及它对于我们来说有何特殊意义。

IT 三大趋势：云计算、移动设备安全与社交网站

随着信息经济的不断发展，几大主要的 IT 趋势占据了主导地位。在接下来的十年中，我们所能看到的最令人振奋的技术发展要属云计算了，它将为企业与最终用户带来巨大的益处。基于云的服务可以帮助企业提高应对不断变化的业务需求的能力，以及按需为最终用户提供计算、解决方案与存储的能力。在考虑到预算缩紧的情况下，随用随付（pay-as-you-go）的模式也十分吸引人，因为它可以更好地预期并控制成本。

第二大趋势是电子设备的使用日益增多。根据 IDC 的预测，到 2010 年底，上网的移动设备数量将超过十亿，而用台式电脑上网的数量约为十三亿左右。很多人认为，云计算与电子设备增多是两种完全不同的趋势，但在我看来，他们密不可分。展望未来，更多的计算能力及信息均在向“云”迈进。云计算可以为这些移动设备带来更多的应用方案及信息，使其功能变得更加强大。

第三大趋势便是社交网站的流行。社交网站具有真正的商业价值，它让我们能够更有效地分享信息，并相互协同起来。但当我们把更多的信息放在网络上或者“云”中时，我们必须进行风险管理，不管是针对隐私还是数据。

这些趋势背后存在着千丝万缕的联系，不管是云计算、电子设备还是社交网络，它们都是快速分享信息的方式。

需要新的安全方法

以上的几个趋势将促使 IT 向云计算方向发展，云环境则需要新的安全方法，毕竟安全是首要的

关注点。

首先，从基础架构角度来看，安全需要贴近应用与数据。在共享服务架构中，如果只是简单地保护云周边、数据中心，甚至是单独的服务器或存储阵列，安全性是不够的。

其次，当今 IT 世界最大的难题之一便是保护与管理非结构化数据。内容感知技术可以帮助企业更好地实施数据治理策略。能清楚地知道有哪些数据存在、谁拥有这些信息以及它如何被使用是至关重要的。如果你不知道信息属于谁或它是如何被使用的，那么，将很难建立起一个合适的治理策略。

另外，确保云安全还需要安全和法规遵从的技术，以帮助使之不断演进，从而提供增强的可视性，这将提高服务提供商或服务消费者模式的信心。除了口头保证或书面的服务等级协议（SLA），服务消费者还需要实时了解云供应商的安全状况，使他们能够相信，他们的信息在根据其治理策略而受到保护和管理。

最后，基于云的安全服务不断发展，它将能够降低 IT 部门管理安全的复杂性，使他们更专注于与业务相关的问题。但是，随着云计算的不断演进，企业可能会选择最适合他们的模式，可以为他们创造不同情景的模式。因此，企业内部的安全工具与基于云的服务之间的互通性十分关键，这样它们可以协同作用，从而最大限度地发挥二者的优势。

熊猫安全:真云不怕“毒”炼

来源：比特网

您的防病毒软件可以无需本地病毒库，直接通过云安全技术检测超过 4000 万种病毒吗？您的杀毒软件接入互联网云端后，可以检测出更多的病毒吗？您的企业级杀毒软件可以无需任何本地服务器完全通过互联网云端来管理吗？

目前市场上“伪云”泛滥，各家都在炒作自己的“云安全”，究竟什么是“真正的云安全”呢？熊猫安全认为，只有彻底解决以上几个基本问题，才是“真正的云安全”，才是“真云”！

由于传统杀毒软件受到用户计算机硬件性能的限制，通常在本地只能存放百万级的病毒库。只有通过真正的云安全技术才能检测超过 4000 万种病毒的历练。而根据 IDC 预测：“到 2013 年云安全市场将会增加 300%”，并大胆地推断，只有在这一领域不断推进的企业届时才能生存下来。

根据全球知名咨询机构 Yankee 集团 2007 年初的研究：“到目前为止，熊猫安全是唯一一家具有云安全的大型安全公司。”熊猫安全作为云安全的倡导者与领导者，早在 2006 年底率先提出了云安全的概念，2007 年将其云安全技术成功应用到全线产品中。

据悉，熊猫安全的 PandaCloud Office Protection——PCOP 是一种基于 Web 的可订阅式服务，

它不但可以减少中小企业在防病毒上的硬件投入、人员费用和管理成本。而且也可以为中小企业提供基于 Web 的服务，方便安全服务提供商为中小企业提供更好的服务。

熊猫安全中国区 CEO 金锴介绍说：“PCOP 采用熊猫安全独特的云安全技术——综合智能技术，可以深度检测恶意软件，使得每个新文件在收到后的 6 分钟内完成自动分类。综合智能的服务器会自动接收并分类每天收到的 5 万多个新样本。作为一项云安全服务，它提供简单易用的 Web 控制台，让企业随时随地都能管理保护模块，减少操作的复杂性，无需基础设施投资或专业人员，因为所有作业都托管于云中。”

PCOP 包括防护病毒、蠕虫、木马、间谍软件、黑客工具、非法程序、网络钓鱼等。它的主动防护引擎保护中小企业抵御已知和未知的攻击，甚至隐藏的攻击。

金锴说，熊猫安全用综合智能技术对从每台 PC 机收集到的信息进行恶意软件关联性分析，从而不断加强对用户的保护。然而，边界防护硬件设备可以有效地防止基于互联网的威胁，保护企业的内部网络。但是不同类型的威胁最好由不同类别的专用设备来进行处理。利用 PCOP 与熊猫安全网关 GDP9000 的完美组合，可为各种规模的公司提供高度可扩展而且全面的网关级防护，免受各类基于内容的威胁。

熊猫安全网关是一款高性能的内容安全管理(SCM)设备，为企业的边界网络提供有效的防护。它针对来之互联网的威胁提供了强大而且功能丰富的边界防护。它的防恶意软件、反垃圾邮件和 Web 过滤功能，可以完全满足网络

管理员的所有安全需求——检测并且清除所有基于内容的威胁、清除垃圾邮件以及确保员工不去访问不恰当的网站。

域名注册机构采用.org 最新安全性措施

来源：新浪科技

北京时间 6 月 24 日凌晨消息，据国外媒体报道，负责运营“.org”域名的注册机构 Public Interest Registry(以下简称“PIR”)周三称，该机构将推出额外的安全性措施来抵御身份盗窃行为。

业界人士称，.org 域名将是第一种采取额外安全性措施的 DNS(域名系统)，但“.com”和“.net”等 DNS 预计随后也将采取这种措施。目前，共有 800 万个网站使用.org 域名后缀，这一域名在 1985 年被采用，是互联网上最早的 DNS 之一。使用.org 域名的通常是非营利机构，许多信用社的网络银行服务也使用这种域名，因此这种域名经常成为那些意图窃取银行帐号或网络捐款的骗子的目标。

业内咨询机构 Javelin Strategy and Research 在其“2010 年身份欺诈调查报告”中预测称，单单是在美国市场上，去年身份盗窃案例就已经增加了 37%，对 1100 万人造成了影响，所带来的损失总额

高达 540 亿美元。另据非营利周刊《慈善编年史》(The Chronicle of Philanthropy)统计的数字显示,目前美国每年有 10 亿美元以上的捐款是通过互联网进行的;在 2005 年到 2006 年之间,这一数字增长了近 40%。

ICANN(互联网域名与地址管理机构)在为期一周的布鲁塞尔会议上表示,最新的 DNS 安全性措施将对.org 网站上的数据来源进行鉴定,以确保这些数据的完整性。ICANN 总裁罗德·贝克斯托姆(Rod Beckstrom)称:“简单来说,DNS(安全性措施)允许互联网用户确切地知道他们曾到过自己想去的网站或位置。”

从实际效果而言,新措施给有效数据提供了一把“锁钥”,确保这些数据在传输过程中没有被篡改,这种安全性措施已被使用巴西、保加利亚、捷克共和国、波多黎各和瑞典等国家域名后缀的网站所采用。PIR 首席执行官雅莱柯萨·拉德(Alexa Raad)称,互联网域名注册机构 Comcast 和 Go Daddy 都已经同意实施这种额外的安全性措施,预计其他注册机构随后也将采纳。

对于普通上网者来说,当其登陆.org 网站时不会发现任何改变。使用.com 和.net 后缀的网站预计将在 2011 年第一季度以前采用这种额外的 DNS 安全性措施。

专家为你解读 高校 Web 安全“新药方”

来源:中国信息安全博士网

近年来,高校互联网应用的普及,在便利学校管理与增强社会服务功能的同时,也招来了大量或“黑”或“红”的不速之客。特别是应用系统 Web 化之后,黑色产业链也开始瞄准校园网,高校网络以往的安全“免疫系统”已经明显失去了效力,用户急需方案商开出更有效的安全“新药方”。

近几年来,各大高校为了增强信息化系统的社会服务功能和访问的便捷性,都在向 Web 应用模式转型。为了保证这些 Web 应用系统的安全,大多高校网也都部署了 SSL 安全代理、防火墙、IDS/IPS,以及软件防火墙、防病毒这类安全设备。但是,高校网遭遇的恶性攻击事件不仅没有因此减少,反而还出现了大幅飙升的趋势。

“老三样”安全防护失效

“湖北多所高校网站遭攻击 考生录取记录被篡改”;“北大网站遭黑客篡改 假冒校长抨击大学教育”;“黑客攻击清华大学新闻网 捏造顾秉林粗俗讲话假新闻”;“知名高校挂马现象严重 考生面临安全风险”。如今,类似的高校网“中招”事件比比皆是,这些网络攻击不仅能轻易穿透高校网的安全屏障,还能在后台随便篡改数据。据杭州安恒信息技术有限公司技术总监范渊介绍,这些幕后黑手正是通过 Web 应用系统的漏洞,越过了高校网的安全防护体系。

“事实上,当前以 Web 应用系统为跳板,入侵服务器甚至控制整个内网系统的攻击行为已成为

黑色产业链最普遍的攻击手段。据一些搜索网站的统计，目前 70% 以上的攻击行为都是基于 WEB 应用系统的。”

在范渊看来，校园网之所以在遭遇攻击后损失重大，主要是因为大部分学校的对外服务网站都与其内网系统相关联，攻击者更容易以应用服务器为跳板实现对校园内部系统的入侵。所以，对高校用户来说，因此导致信息泄露、信息被篡改及重要数据被破坏等损失的几率就更高。所以，高校网信息安全的第一道防线，其实应该是基于 WEB 应用系统的安全防护。

“很多用户认为，在网络中部署多层的防火墙，入侵检测系统(IDS)，入侵防御系统(IPS)等设备，就可以保障网络的安全性了，就能全面立体的防护 WEB 应用了。但是，为什么攻击事件依旧不断发生，并不断造成损失呢？其根本的原因在于，传统的网络安全设备对于应用层的攻击防范，作用十分有限，如今的这些攻击正是基于 WEB 应用的攻击。”

范渊告诉记者，目前的大多防火墙都是工作在网络层，通过状态防火墙保证内部网络不会被外部网络非法接入。由于所有的处理都是在网络层，所以应用层攻击的特征在网络层次上是无法检测出来的。而 IDS、IPS 这类设备对于未知攻击，和将来才会出现的攻击，以及通过灵活编码和报文分割来实现的应用层攻击，IDS 和 IPS 同样无法提供有效的防护。而软件防病毒、防火墙产品，一般采用被动的检测机制，只能检测已知病毒或木马，并且无法识别外部的正常访问请求。

可见，基于“老三样”安全产品的 WEB 应用系统安全解决方案，对应用层的安全问题并不适用。高校用户就算采购更多这样的安全设备，也无法有针对性的解决他们现在的安全问题。这也是当前一些方案商在提出解决方案后，遭遇出局命运的原因。

多层防护铸就铜墙铁壁

范渊表示，应用层的安全问题更为复杂，和传统的解决方案相比，“新药方”需要具备综合治疗的效应，单一的产品很难彻底帮用户解决问题。

“所以，我们的解决方案是由 7 大子系统构成的，目标是构建一个整体多层防护系统。它包含网站 WEB 应用弱点扫描子系统、网站防攻击子系统、网站防篡改子系统、网站应用安全审计子系统、网站数据库弱点扫描子系统、网站数据库安全审计子系统总共 7 大部分，从各个层面和各个角度为网站系统建立起一个立体的防御体系。”

范渊解释道，网站的整体安全检测主要依靠网站 WEB 应用弱点扫描子系统和数据库弱点扫描子系统来完成。通过 WEB 应用弱点扫描子系统，可以快速检测网站可能存在的 SQL 注入、跨站脚本、表单绕过等应用弱点，并根据检测结果有针对性的采取安全加固措施。而通过数据库弱点扫描子系统，就能快速识别数据库系统存在的补丁状况、弱配置状况等安全隐患，再通过有效应对去尽可能防范对后台数据的入侵。

而监控审计也是防御 Web 攻击的关键。通过网站应用安全审计子系统和网站数据库安全审计子系统的协作。安恒的解决方案可以深度检测所有 HTTP 访问数据，并实现对网站访问的 7x24 小时实时监控，对检测到的异常访问和攻击行为，系统都会报警、通知用户，协助网管人员第一时间采取

安全应急措施。而且，系统的日志功能，也为安全审计提供了基础。网站数据库安全审计子系统同时在帮助用户检视所有的针对数据库服务器的访问，除了日常的 SQL，还包括通过 FTP、TELNET 等其他的访问方式，实现了对后台数据库日常操作的监控、危险操作控制以及安全事件的追溯。

安全远程访问：为企业应变计划填补空缺

来源：eNet 硅谷动力

如果有机会回到本年初查阅全球 500 强企业的公司应变计划，估计没有哪家企业会把冰岛火山爆发导致业务瘫痪预计在内，然而冰岛埃亚菲亚德拉火山在 4 月 14 日喷发，浓密的火山灰笼罩欧洲空域，令航空交通停顿 6 天，大量旅客被滞留外地，出差在外人员不能及时回到公司工作，以至商业的正常运作受到很大程度的干扰。

这次火山喷发实属罕见之极，促使企业不得不重新审视其应变及业务持续计划，而安全远程访问可能是其中一个应对方案。

Check Point 安全顾问吴航表示，对于多数企业而言，员工及合作伙伴能够进行安全远程访问应被视为现代应急方案的核心，在办公场所不能正常使用，或员工未能按时到办公室上班时，业务仍然维持正常运作。

面对突发事件，企业需要安全、灵活的远程办公解决方案，它应该可以快速扩大使用规模，不需经常支付昂贵的使用权认证、维护及支持服务。后者尤为重要，因为在正常情况下，远程访问解决方案的使用程度不会达到极点，因此在控制成本及迅速提供高度可用的远程安全访问两者间要取得平衡。

对用户数量的考量

企业要考虑的第一个课题是预计在紧急情况，它需要为多少名远程用户提供支持。基于客户数量的 VPN 解决方案没有足够的灵活性，因为在使用之前用户需要取得软件使用许可认证。

一般来说，公司只有管理层和高级员工才在笔记本电脑或家用电脑中装有 VPN 客户端。然而在突发事件爆发时，其它员工并未安装 VPN 客户端，那么企业将如何保证所有员工能够进行安全访问？

因此，灵活的安全远程访问必需适用于全面管理设备（公司笔记本和智能手机），以及不被管理、无 VPN 的设备（家庭及合作伙伴的电脑以及公共网吧）。

这个方案必需可以对于用户的访问权限进行严格管理，根据用户的不同需要、信任等级、设备种类和安全级别来授予或限制访问权限。

对端点的考虑

另外，传统的 VPN 解决方案要求每个远程用户 PC 装有最新的防恶意软件和最新的软件补丁。

否则，恶意软件将远程攻击企业网络，木马病毒将在终端电脑上劫取机密信息。

因此，解决方案需要在远程访问结束时，使用数据加密来阻止有用信息停留在端点，并清除缓存，消除电脑上所有的工作痕迹。它还应提供安全保护，使电脑免遭外界及用户本身的错误操作和疏忽造成的威胁，而这些动作必须隐秘进行，且不干扰用户的使用体验。

如果使用传统安全产品，例如在企业大数的笔记本电脑中安装如独立 VPN、防病毒软件、数据加密、个人防火墙和入侵防护，这将会十分复杂，而且价格昂贵。因此，企业需要另一种远程访问方式，以降低应急方案的复杂性和成本开支。

把个人电脑放进 U 盘

吴航表示，Check Point 新近推出的 Abra 方案可能是企业寻觅的答案，随着千兆 U 盘的问世，Check Point 实现了“把个人电脑放进 U 盘”的构想。Check Point Abra 解决方案可把一台普通 PC 变为受到全面保护的公司电脑。

该解决方案采用虚拟技术，将 Abra U 盘插入任何电脑的 USB 接口，就能为用户生成虚拟桌面电脑。它将主机转变为可信赖端点，使用户能够进行安全远程办公，并提供 VPN 连接，使用户能够安全访问公司网络。用户可以使用在办公室相同的 Windows 桌面，使用相同的快捷方式和文件夹完成工作。Abra 操作非常简单，用户只须插入设备，输入密码，便可使用。

用户使用主机 PC 对数据进行操作，但数据被保存在 U 盘的安全虚拟空间中。这就保证了本地数据和企业网络的完整性，防止恶意软件和黑客的入侵，及数据丢失和盗窃。换言之，没有数据会被写入主机，主机的恶意软件也不会进入安全的虚拟工作环境。

当用户结束工作，安全虚拟工作环境就会消失。Abra U 盘具有自动硬件加密功能，所有数据都被加密写入闪存中，工作痕迹或 VPN 连接将不会存在。即使停止使用解决方案，所有的信息都自动加密存储在闪存上，因此如果该设备被盗，用户信息、文件夹、文件和其他机密数据都仍会受到保护。该设备接受中央管理，符合公司政策，丢失时可重置。

此类安全虚拟工作环境解决方案解决了应急方案中远程访问成本、复杂性和规模问题。它使公司能够为员工及合作伙伴提供持续、可控、安全的网络访问，并与主机完全隔离。

该解决方案也比购置大批笔记本电脑更加简单、节约。Abra U 盘体积纤巧，员工可以轻松将其带往任何地方，企业 IT 部门不用管理员工大量远程访问及大批端点的麻烦，且始终保护机密数据的安全。

云端安全：可信任的云计算前端让性能可靠

来源：赛迪网

云计算为组织提供兼具可扩展性和成本效益的灵活的 IT 新选择，但要实现云服务的全部优势，企业必须信任这些新服务的安全、策略和流程。企业要扩展外围的 IT 安全，必须首先建立一个可信任的云计算前端：提供安全保证、管理、控制以及可靠的性能。

组织考虑采用云技术——但他们能够信任云吗？

越来越多的组织转向云计算。据分析机构评估，云计算市场规模可达 420 亿美元，至 2013 年，仅软件即服务(SaaS)市场即可增长至 160 亿美元。某些组织是受到云计算显著优势的吸引而转向云计算，而某些组织是发现其竞争对手通过云计算赢得了优势，进而迫于压力也开始采用云计算。对于很多组织而言，这两种力量都起到了一定作用。

几乎每个 CIO 的解决方案候选列表中都包括一个云计算选择，因为云计算能使企业提高 IT 的质量和灵活性，而 IT 正是其业务赖以运行的关键。云应用程序、平台和基础架构服务可以扩展数据中心的功能，同时有效利用资源，降低 IT 部门的总拥有成本。云服务采用“即用即付”模式，使组织能够从小规模开始快速扩展，既不牺牲服务质量，也不要求在基础架构上投入大量初始投资。

云计算是现今 IT 最重要的趋势，而且可能在未来数年继续保持强劲态势。然而，这个行业仍处于发展初期：平台不完整，安全措施尚未成型。IT 管理者不能忽略云技术——但尚不能充分信任它。

信任第一

尽管企业认可云计算的潜在优势，但他们不愿意将所有关键处理或数据迁移到云中。并不是说云技术的固有安全性优于或逊于企业现有环境，关键在于前者采用一种截然不同的方式，特别是对第三方的依赖。

在接受云计算之前，组织需要要求服务供应商确保其关键资产的安全。但企业应该知道，云安全并不是一种简单的“全部肯定或全部否定”的选择：他们可能必须在开放性和安全性、控制与可用性、灵活性与风险管理、过程与实施之间作出权衡。

在依赖 SaaS 和云服务来提供计算能力、存储和关键业务应用程序之前，组织需要明白这一点：自己的策略仍适用于云中的资源，并且能够审核云策略的实施。信任还要求服务等级协议(SLA)保证可用性、可靠性和业务连续性。而且组织应该要求云供应商解决新出现的数据泄漏问题，包括因多租用和云运营商的访问而导致的此类问题。当企业从仅使用一种云服务迁移至使用不同供应商提供的多种云服务时，他们必须处理与多个运营商合作而产生的所有问题，而每个运营商具有不同的基础架构、运营策略和安全技巧。在如此复杂的信任需求的推动下，产生了对可信任云计算前端的需求。

可信任的前端：概述

可信任的云计算前端是一种安全和信任中介服务，它面向多种云服务提供单一便利的入口，鼓

励管理员、员工和业务合作伙伴采用云应用程序与流程。它可以改进组织原有的安全，同时使安全的实现比以往更加简单。对于企业而言，可信任的前端就是一个符合开放标准的 API。对于云供应商而言，它支持多种接口，有助于业务合作伙伴的集成。而双方都无需了解：可信任的前端如何避免企业及其云供应商摆脱实施强大安全措施而导致的高度复杂性及高昂成本，以确保云用户、应用程序和数据的安全。

对于多数组织，选择经认可的可靠服务供应商(或"信任供应商")提供安全与信任中介服务是为云创建安全前端的最佳方式。在选择可信任前端供应商时，组织应评估他们是否已妥善解决保证、管理、控制和可靠性能的关键问题，并确立一个度量标准，以帮助确保组织在上述领域中获得相应的投资回报。

安全保证决定门的开启

信任供应商应通过严格的用户认证和授权来保证安全，并额外考虑高优先级或高风险用户的安全以及远程访问使用案例的挑战。在所有情况下，供应商都必须证明自己能够根据企业的访问策略拒绝未授权用户的访问。尽管可信任的前端主要依赖现有流程和资源，但它可以通过动态插入例如多因素认证等其他安全层来提高安全性。

组织应该考虑可信任前端的供应商是否提供查核例如笔记本和智能手机等用户设备的信任度的能力。基于恶意软件的威胁已经影响消费者多年，最近的公司攻击已经表明，终端保护不会保护企业用户设备免受外部攻击。信任供应商应该保护和监视用户设备，并评估是否许可他们访问机密的云资源。

由于可信任的前端能为云供应商提供安全最佳实践，所以行业可以形成一致的类似于信用卡行业的 PCI 标准的云安全标准。然后供应商可以根据这些标准要求 SaaS 和平台即服务供应商取得认证。与此同时，信任供应商可以独立提供安全认证服务和漏洞评估服务。

管理使企业重掌控制权

尽管云应用程序拥有户内应用程序所不具备的优势，它们也可能由于支配和管理用户、应用程序和业务流程而打乱组织的模式。组织应该对任何 SaaS 或云服务供应商的安全管理过程和功能进行评估，确定它们是否充足且成熟，以及是否与组织自有的信息安全管理实践保持一致。

对于多数企业而言，可信任的前端会与公司目录和元存储库集成起来，支持在外围形成一致的管理、认证与授权。其他企业可能会选择一种更为简单的策略实施方法，即依赖于自动化用户配置和取消配置。

对于传统的身份与访问管理平台，可信任的云计算前端类似于访问请求交换机/路由器，同时发挥着外部策略实施代理的作用。作为身份中介和授权代理，在利用组织内部例如企业域控制器等信任源或例如 Google 或 PayPal 等外部身份供应商服务的 bootstrap 凭证和认证时，可信任前端应避免发生凭证泄漏。因此信任供应商应遵守例如 SAML、OPENID、OAUTH 和 XACML 等标准，以避免日后发生锁定。

控制是合规性的关键

信任供应商不仅必须提供保证、管理和可靠性能，还必须全面跟踪、审核和报告他们提供这些服务的效率。对于每个单一访问事件，供应商应该能够监视并报告访问者、访问内容、访问方式、访问时间和访问位置等信息。

可信任的前端简化审核跟踪和合规性报告，提供整合访问事件日志的绝佳机会。审核者更容易检查跨所有云资源和所有用户的法律、法规和规则(例如 SOX、HIPAA、PCIDSS)的合规性。

可靠性能推动业务连续性

组织必须对其信任供应商充满信心，相信他们能够提供完全符合 SLA 的云资源访问。组织还必须调查信任供应商是否符合连接、冗余、故障切换、灾难恢复和防范 DDos 攻击等方面的行业最佳实践。

云供应商合作伙伴和组织需要讨论并商定 SLA 可靠性标准以及根据所有 SLA 进行监视和报告的流程。可信任供应商服务可跨企业所依赖的所有云服务提供整合的 SLA 监视与报告。这可以提高可见性，降低管理多个独立云的操作复杂性。

结论：行业领先者努力勾画信任的蓝图

确保跨多用户及云资源的严密安全性与灵活性是一个前所未有的挑战，多数组织都不具备这种挑战所要求的专门技能，而且也没有时间去培养这种技能。因此一种新类型的服务供应商应运而生来应对这种挑战，他们创建可信任前端，以新的方式重新集成最优质的应用程序、数据和用户，使组织不仅能够保持按需模型的灵活性，也能够将访问策略和安全控制扩展到云中。通过选择使用这样的服务供应商，组织可以引入最佳实践，在复杂 IT 环境内实现可信赖的安全性。

黑客攻防

苹果偷偷发布补丁修复一个木马安全漏洞

来源：赛迪网

据国外媒体报道，安全公司 Sophos 的分析师说，他们发现一个偷偷发布的苹果杀毒软件的补丁。苹果本星期发布的安全通知中没有提到这个补丁。

在分析了这个补丁之后，研究人员发现 OSX 中的一个 XProtect.plist 文件的更新。这个补丁将阻止 4 月份首次发现的 HellRTS 木马程序。这个木马程序假冒 iPhoto，但是，实际上是让攻击者控制被

感染的系统，利用被感染的系统发送垃圾邮件和参加分布式拒绝服务攻击。

Sophos 高级技术顾问 Graham Cluley 在博客中说，遗憾的是许多 Mac 机用户忘记了自己的计算机上能够有安全威胁。当苹果像这样偷偷地发布杀毒软件更新，而不是通知大众它做了什么事情的时候，这种做法是没有帮助的。

你一定会感到奇怪，苹果像这样偷偷地发布杀毒软件的安全补丁是不是由于营销的理由。“嘘，不要告诉人们我们必须防御针对 Mac OS X 操作系统的恶意软件。

与 PC 平台相比，苹果系统目前的恶意软件数量是非常少的。但是，专家们警告说，苹果用户对于安全是自鸣得意的。苹果商店的给用户的忠告中似乎就反应了这个问题。

安全厂商常漏掉新恶意软件

来源：赛迪网

据国外媒体报道，新研究进一步证实了安全软件公司在恶意软件数量爆炸性增长的今天显得无能为力。根据来自负责测试安全软件套装应对新发恶意软件情况的 NSS 实验室的最新报道，主流厂商的产品平均要花费两天的时间来阻止一个恶意网站，而每天大约有 5 万个新的恶意软件出现。安全厂商分享恶意软件样本，但是如果没有一个厂商发现某恶意软件，那么它就会悄无声息的进行攻击，窃取数据。

NSS 实验室是一个独立的安全软件测试机构，不接受厂商的现金资助，因此测试结果比较客观准确。它公布表现最差的产品，并将参加测试的产品分为三类：推荐，一般，警示。它将 AVG 和 Panda 公司的产品列为“警示”，完整的测试结果包含在 NSS 的报告中。此次测试还包括 Eset，F-Secure，卡巴斯基，麦咖啡，Symantec，趋势等公司的产品。

内部用户帐户控制：谁来监督“监督人员”？

来源：比特网

问：我在一个安全部门工作了几年，现在，我们考虑增加一名初级管理员。我想给这个人的一个任务是安全管理，目前负责涉及 IT 运营和商业用户方面的工作。我有两个问题：1)对帐户进行集中管理是好的做法吗？2)谁来监督“监督人员”？换句话说，如果我的工作组有能力创建帐户，应该由谁来监督我们，以确保我们不会做任何不恰当的操作，例如创造假帐户，窃取数据，并在之后

立即删除该帐户？

答：很高兴听到你的工作终于有人可以分担了。在你的问题中，你没有提供任何关于你机构的组织信息，所以我不得不说，你第一个问题的答案是“看情况”。凭借经验，对用户帐户进行控制的做法是尽可能地了解用户：这意味着你必须能够验证请求者是否是真正提出请求的那个人，以防止他人在未经用户许可的情况下创建帐户。如果你与请求者位于同一常规地理区域或可以很容易地联系到请求者，并且可以证实用户或者用户的经理提出了请求，那么此时进行集中管理是可行的。然而，如果在语言沟通上存在问题，你没有一个是验证用户请求的简单方法，或者你有高度分布的、或政治性的、或孤立的商业模式(siloed business model)，那么分布式的管理会更合理。

至于由谁来监督“监督人员”？这个问题已经讨论了多年。正如在另一个问题中所提到的，责任分工(SoD)的最佳实践验证了一个帐户管理员不应该拥有建立帐户的能力或特权(正如你上面所提到的原因)。因此，为了监控这些活动，在机构内部设立审计职能很重要。不管它是隶属于法律部门、监察部门还是能监测出非授权流量的网络工程部门，是否配备审计职能是一个跟机构息息相关的决定。如果审计小组方案由于成本、经验不足、机构规模、政治等原因而不可行的话，那么唯一的方法是由人力资源部门对拥有审计职能的人员进行周期性的背景核查。他们会留心犯罪分子和财务信息，以保证不会出现授权用户因外界压力所迫而做出非授权操作的事件。由于赌博、离婚、抵押债务等问题所带来的压力，出色的管理员已经开始变质了。同时也要留心工作人员的个性特点，你所希望的应该是让喜欢自己的工作、与他人和谐相处、真正诚实、快乐的人去做这项工作。有心事的管理员总归不是一个好的迹象。

最后一点我想说的是，美国政府的 CERT 团队已经就“减少内部威胁问题”制定了许多很好的标准。你应该去访问他们的网站，了解所有危险的管理员活动的潜在前兆以便做好警惕。祝你的新管理员好运，如果一切顺利的话，你现在可以去度假了，我敢肯定你一直在推迟这次假期。

Wi-Fi 加密技术屡屡遭破

来源：网界网

针对为何 Wi-Fi 蹭网器设备能形成产业化、使用范围越来越广一事，有业内人士介绍说，这主要是因为 Wi-Fi 本身存在安全漏洞，早先 Wi-Fi 的安全机制 WEP/WPA 早已被破解，而升级后的 WPA2 同样可以被破解。

所谓“蹭网”就是指在有无线路由器覆盖的区域，用一个特殊的设备破解指定无线网络的接入限制。也就是说在别人不知道的情况下去共享别人的网络。这个“特殊的设备”就是“蹭网卡”或者“蹭网卡器”。

此前，市场上甚至已出现 Wi-Fi 蹭网器分等级，零售价从 80 元至 280 元不等，这严重威胁到 Wi-Fi 用户的安全，使得 Wi-Fi 安全问题再度引发关注。

对此，有业内专家介绍说，Wi-Fi 安全机制一直在升级，Wi-Fi 以 IEEE 802.11i 作为安全接入标准，IEEE 802.11i 包含了三种安全机制：WEP、WPA 和 WPA2，其中，早期是使用 WEP/WPA 作为安全机制，但已被证明存在严重安全漏洞，目前网上到处流传着破解上述 Wi-Fi 安全机制的方法。

WPA2 是 WPA 的升级版本，今年，Wi-Fi 联盟发布了 Wi-Fi 最新的行业安全路线图，并宣布：将全面摒弃 WEP/WPA，推进 WPA2 这一新的安全机制，企业和家庭用户的 Wi-Fi 产品将陆续支持 WPA2。但从国内 Wi-Fi 蹭网器产业化及技术水平来看，实际上，WPA2 也将很快被破解，否则的话，国内 Wi-Fi 蹭网器很难推广并在用户中广泛使用。

几年前，Wi-Fi 联盟针对存在严重安全漏洞的 WEP，发布升级补丁版 WPA 时，也曾对外宣称：WPA 将在可以预测的将来满足制造商以及消费者双方的要求。但很快，WPA 即告破解。

数据丢失防护部署中的五大安全技巧

来源：网界网

部署终端数据丢失防护可能是所有 DLP 项目中最令人恐惧的一步。这里有五个技巧可以帮你避免 DLP 部署中常见隐患，同时成功地保护企业数据。

这里有五个技巧可以帮你避免常见的隐患，同时成功的保护企业数据：

1.在静态工作站镜像上测试是非常不错的，但数据丢失防护的大多数问题出现在首次将其部署到使用数据的用户。在你推出部署数据丢失防护解决方案的第一个部门确定一些关键用户，根据需要对他们进行培训，并在测试阶段与他们密切合作。通过关键用户的帮助，可以避免非技术业务部门测试中出现的问题，也可避免部署中没有任何用户反馈的情形发生。

2.确保你的目录服务器是最新和准确的(这实际适用于任何形式的数据丢失防护部署)。如果你试图根据计算机组而不是用户角色来管理策略，可能会产生策略冲突(特别是当用户发生了变动)。大部分组织将他们的数据丢失防护策略设计成根据用户角色应用不同的策略，例如，财务部门就比客户支持代表有更多的自由来处理财务信息。即使一个计算机组已经映射到一个业务单元或该业务单元中的一个特定用户，在下次更新时可能会破坏该策略。依据用户以及组或者角色要比依据计算机来管理好得多，即使这意味着你首先需要花一些时间对你的目录服务器进行调整。

3.建立适应用户在你的数据丢失防护网络内和非受控的网络之间变化的策略。例如，在你的网络内有一个数据丢失防护策略检测和阻止你的客户数据库中的信用卡号传输，当终端离开公司网络时，在终端上的策略发生变化，允许正常的使用信用卡。这是完整的数据丢失防护工具和其终端代

理诸多特性中的一个，但不是全部。部分文档匹配和数据库指纹策略非常占用内存，远远超过了用户的笔记本和台式机的能力(假如用户在数据丢失防护之外还要处理其他的事务)。切换一个模式匹配策略，例如正则表达将会增加误报，但会减少对电脑性能的影响。你也可以设置策略切换到监控/警告模式，而不是阻塞模式来进一步减少对用户的影响，虽然安全风险较高。

4.首先关注终端发现和 USB 保护。在一系列的终端数据丢失防护工具中，发现(查找本地硬盘上的敏感信息)和 USB 监控/阻塞是最重要的两个功能。帮助跟踪用户在受认可的企业应用程序之外获取敏感信息，和在本地存储或共享敏感信息的行为也是终端数据丢失防护的重要特征。一旦启用终端发现，选择增量扫描(如果你的产品提供了该功能);没有人希望他们的电脑因为每周三午间的杀毒扫描而突然停止，而每周四又进行数据丢失防护扫描。同时确保你扫描的位置不只是用户的默认文件目录，因为他们很少会把所有文件放在同一个位置。最后，如果你允许用户使用本地的微软 Outlook PST 文件，确保你的产品可以扫描 PST 格式的内部去捕获移动到本地存储的邮件。

5.慢慢来，逐步推出代理和策略。在完成你的初步测试后，一个组一个组的推出那些策略来确保产品具有良好适用性，这样以来不会给你的事件响应团队造成太大压力。当用户第一次开始使用数据丢失防护时，几乎每一个 DLP 客户都会出现大量的策略违反报告，直到用户自我训练到可以更好地管理受保护的信息之时这一情况才会得到缓解。这个过程应该如下：在一个小的用户组中执行一个策略，然后扩大这个策略(和代理安装)持到达到你设定的覆盖范围。一旦第一个策略工作良好，用同样的方式推出第二个策略，虽然你现在不必担心安装新的代理。

虽然这些提示不是部署和管理终端数据丢失防护的所有方面，但仍有助于避免一些最严重的缺陷，并更快的实现你的新工具带来的安全价值。

21 世纪经济报道：信用卡存危险盗刷暗门

来源：世纪经济报道

每张信用卡，都可以轻松盗刷，只要你懂得利用现行第三方支付系统中的一个小小的漏洞。

比如，只要打通了信用卡“离线支付”和“过卡支付”——两个原本并行无交集的系统，你就可以从别人的银行信用卡中把钱划走。

这些钱，将如同多数的信用卡离线支付一样，依次经过发卡银行、银联、收单银行、第三方支付机构之手，抵达你的账上。

当然，信用卡持卡人可能总有一天会发觉钱不见了，但他也将无可奈何，因为这种无头公案，最后总是找不到负责的人。从发卡银行、银联、收单银行，到第三方支付机构，都只会把他当皮球踢。

于是，这个可能酿成金融风险的漏洞迄今没有完全补上。于是，被“盗刷”的钱仍在源源不断的流入发现这玄机的精明鬼手里——这些第三方支付机构的签约客户，至今还没有谁被投入监狱。

这堪称世界上最安全的犯罪。直到最近的这一周，这一切混乱才终于引来一场监管风暴，矛头指向给上述盗刷造就风险缺口的第三方支付平台。

6月21日，央行发布《非金融机构支付服务管理办法》，要求非金融机构必须在申请和获得相关牌照后，方可从事支付服务。

“(第三方支付)这个领域新的风险隐患相继产生。”央行相关负责人在解释对第三方支付实施准入制的背景时说，比如支付服务相关的信息系统安全问题等。”

那一串数字里的秘密

陈方(化名)是那些莫明其妙的买单者之一。

这位普通的工薪族，平时使用信用卡的次数很少，每个月都细心地核对对账单。这让他很容易发现，在自己招商银行信用卡的9月份扣款中，多出了记忆之外的一笔，金额300元。

陈方给招商银行信用卡中心拨去电话。几番沟通后他获知，这笔钱由网银在线为“乐在上海”代扣走了。

陈方回想起来，一个多月前，他在街头遇到“乐在上海”的摊点，工作人员热情地向他推销一种本市消费折扣卡，并许诺30天试用期过后不续订可自动取消，然后递给他一张详细的个人资料登记单。

“要填信用卡卡号啊？”陈方有点起疑。

“放心好了，没有密码我们划不了款，这只是个资料搜集。”工作人员说。

陈方想起自己的信用卡密码，放下心来，把卡上的数字抄在单子上。

后来的事表明，正是这串“数字”，让陈方的信用卡成了“乐在上海”的提款机。

随后，在与“乐在上海”、招商银行沟通均无果后，陈方联系了本市电视台新闻热线。很快，一直声称“持卡人责任自负”的招商银行，归还了陈方上述扣款。

记者了解发现，上述款项，依次经过招商银行(发卡银行)、银联、网银在线(第三方支付平台)、收单银行，抵达“乐在上海”账上。

“我们是这件事的受害者，垫付了这笔钱，现在只能计入坏账。”招商银行信用卡中心宣传策划室副经理丁诗妮表示。

“我从没听过这种案例，也不知道问题出在哪。”中国银联一位相关负责人说：“银联只是跨行信息转接，网上银行的控制由各银行控制，或者第三方支付机构。”

“我们不会插手。”网银在线人士对本报记者说：“风险控制是银行的事。”

至发稿时，“乐在上海”方面未对记者的求证作出回应。

记者了解发现，案例中的收单点签约，是由第三方支付机构——网银在线完成的；相应的风险控制漏洞，亦由此而来。

危险的“第二种密码”

“中国信用卡使用规则和美国等地的通行规则不一致，造成了操作上的混乱。”一位中国银联美国分部人士告诉记者。

信用卡的使用，分为“过卡交易”和“离线交易”两种。前者由持卡人持信用卡在商场、超市等“实体店”的POS(销售终端)机“刷卡”，并签字授权，完成交易。

离线交易，则常见于酒店、航空公司销售中心、公司财务等，同样通过POS系统，提供信用卡账号及其验证码，即可完成交易。

在美国等信用卡起源地的多数西方国家，信用卡不设密码，两种交易方式中，交易凭证仅为签字或验证码。

而在中国，根据本土消费习惯，银行往往鼓励持卡人给信用卡设置密码，来保障用卡安全。

“这种双轨制的信用卡体系下，中国消费者几乎都不知道验证码的存在，更没有相关的风险意识。”一位银联人士表示。

信用卡的验证码，被称为CVV码。它是一串3位数字，由卡号、有效期和服务约束代码，经过发卡银行的编码规则和加密算法生成。

根据信用卡卡种和印刷位置的不同，还有CVV2、CVC、CVC2等，一般印于信用卡卡面、卡号后面。

陈方在“乐在上海”资料单上填下的，正是其招商银行信用卡卡号和CVV码。

在招商银行信用卡中心提供的“信用卡(个人卡)通用申请表”及所附“信用卡(个人卡)通用领用合约”上，都没有任何介绍性、警示性文字涉及CCV码。

在信用卡用户与招商银行签订的唯一一张合约，及银行网站上能找到的“信用卡介绍”中，CVV码丝毫未被提及。

绝大多数的持卡人对CVV码的第一次接触，发生在网络支付的实际操作中——“请输入信用卡卡号后三位数字”。但没有多少持卡人意识到自己正在使用另一种“密码”，它也需要保护。

招商银行不是孤例。记者查阅了建设银行、工商银行等行提供的信用卡章程，上面均无任何CVV码的使用保管提示。这似乎是个没有公开原因的行业惯例。

找不到买单者

正是利用这个惯例，“乐在上海”打通了信用卡中“离线支付”和“实体店”——两个原本并行无交集的支付系统，找到了一条生财之道。

根据其营业执照，“乐在上海”运营机构为上海鹏杨广告有限公司，它的经营范围仅为广告业务。实际经营中，鹏杨广告的主业则为发行“会员消费折扣卡”，向商户收取推广费并向“会员”收取会员费。

身为实体店，“乐在上海”却向网银在线的上海分部，申办了“离线支付”业务。

根据双方签订的服务协议，网银在线在互联网建立支付服务平台，向实体店“乐在上海提供”

电子商务应用服务。

协议期，“乐在上海”可登陆网银在线的服务平台，在“信用卡远程支付 MOTOPAY(即离线支付)”一栏下，登陆被提供的账号，输入客户的信用卡卡号与 CVV 码，便可自行输入金额，进行划款。

“责任就在这个环节，乐在上海的收单银行，对它没有进行应有的实体店资质监控。”丁诗妮认为：“它们乱设收单 POS，授权 POS。”

但招行自己并不在“乱设 POS 的收单银行”之外。

据记者了解，在网银在线向“乐在上海”提供的支付服务中，协议银行包括招商银行、中国工商银行、中国建设银行、兴业银行、广东发展银行、中国银行及 VISA、mastercard 等多个境外银行联盟。

这意味着，几乎中国所有的银行，都被网银在线网罗，会向“乐在上海”们提供收单服务。

而拓展这种收单服务中，第三方支付机构网银在线向市场铺设各类 POS 时，银行与实体店并不发生任何接触，亦没有相关资质审核。

那么，商户资质审核是谁的责任？

在各类离线支付过程，在发卡银行和收单银行之间，至少 1 个或 2 个“中转商”，或是第三方支付平台；或者是第三方支付平台和银联。

在这种“离线支付”产业链中，银联作为信息转接者，的确不涉及商户的资质管理、风险控制。不过，银联亦有子公司进行第三方支付业务，并在该行业市场份额占据前三。

“资质管理的责任，在商户备案的收单机构。”招商银行信用卡中心项目经理张记洲告诉记者：“谁对接商户，就应该谁对这个实体店进行资质管理。”

第三方支付之患

而这个案例中，商户对接的是网银在线。但网银在线并不认为自己应对此事责任。

“我们不会插手，此事由商户与用户协商处理。”前述网银在线总部人士说。

在网银在线与“乐在上海”等各类商户的合约中，此类风险被明文“规避”。按照合约，网银在线不介入商户和持卡消费者或任何第三方之间的交易纠纷，商户应独自承担因其销售的商品或服务引起的各类责任。由于商户责任造成网银在线所提供服务引起的法律上的责任，由商户负责或追究有关方面的责任，与网银在线无关。

至于此种“合约规避”是否合法，并无相关法规明确。

“这是行业通行规则，交易风险是商户的责任。”网银在线人士对记者说：“信用卡欺诈的防范义务在于商户，我们提供信用卡防欺诈系统，给他们一定参考。”

那么，如果不是消费者失误而是商户有意“欺诈”，防范义务又在谁呢？这一点并不清晰。

至于对商户的资质审核，网银在线认为：“乐在上海说他们是网银的合作伙伴，那资质一定没问题了。”

而“合作伙伴”一说，其依据是“乐在上海”自己在某个网页上发布的一段广告。

“这是个行业性问题。”一位第三方支付行业风险控制人士说，作为创新性很大的新兴行业，第三方支付存在不断更新的欺诈手段。

该人士认为，案例的风险控制缺口在于，网银在线作为第三方支付平台，理想状态下，应该保证自己的签约商户不会保存客户核心支付资料，特别是案例中信用卡卡号、CVV 码等。

在支付行业的国际通行认证 PC 中，上述商户资质审核被明确要求。

然而，根据公开材料，网银在线直至 2010 年 2 月，方通过 PCI 认证。

这是否意味着此前的网银在线签约商户，均未通过上述资质审核？而网银在线之外的其他众多支付企业，又有多少仍未经过 PCI 认证？仍不得而知。

或许，央行即将实施的第三方支付行业准入制，可能是目前能寄望的一条出路。

“考虑支付服务的专业性和安全性要求等，(支付服务牌照)申请人应符合内控制度、风控措施等方面的规定”。央行相关负责人在 6 月 21 日表示，将会在随后的管理办法实施细则中，细化技术安全检测认证证明等方面的法规。

企业推荐

艾特赛克（北京）信息技术有限公司

atsec 是一家独立且基于标准的 IT（信息技术）安全咨询和评估服务公司，它拥有丰富的技术经验和较高的国际声誉，为客户提供具有商业导向的信息安全解决方案。2000 年 1 月，atsec 首先成立于德国；随着在国际范围业务的迅速发展，atsec 先后在美国、中国、瑞典壮大。

atsec 秉承专业、诚信、专注、独立的原则，致力于提供高效高质量的国际化信息安全服务。

atsec 的服务

atsec 拥有诸多的成功案例，为客户的质量和安全的提高做出了不可磨灭的贡献，并且超过了客户的预期效果。atsec 测评实验室和服务经过了 ISO/IEC 17025、ISO/IEC 27001、ISO 9001 等标准和规范的认证和/或认可。

atsec 成功地与很多大型机构合作建立、完善并实施管理体系，使其有效整合和符合 ISO/IEC 27001 和 27002 的信息安全管理、基于 ISO/IEC 20000 的 IT 服务管理、基于 ISO 31000 和 ISO/IEC 27005 的风险管理、基于 ISO 9001 的质量管理，以及更多。atsec 咨询顾问已经指导很多的客户成功地完成审计和评估。

atsec 具有丰富的经验提供代码的安全性审查，以及扫描和渗透测试服务。

atsec 是针对支付卡产业数据安全标准（PCI DSS: Payment Card Industry Data Security Standard）授权的合格安全评估商（QSA: Qualified Security Assessor）和授权扫描服务商（ASV: Approved Scanning Vendor），以及支付应用合格安全评估商（PA QSA: Payment Application Qualified Security Assessor）。

atsec 是美国密码模块验证体系（CMVP: Cryptographic Module Validation Program）的测评实验室，提供包括基于 FIPS 140-2 标准的密码模块以及密码算法的测评服务。atsec 也被授权针对 SCAP（Security Content Automation Protocol）和 GSA Personal Identity Verification（FIPS 201）执行软件的验证。

atsec 分别在美国、德国和瑞典获得了认证机构的授权，基于通用评估准则（CC: Common Criteria），也即 ISO/IEC 15408 开展评估工作。atsec 是世界范围内 Common Criteria 评估领域的领导者，特别在开源软件，比如诸多 Linux 版本；复杂的操作系统，比如 IBM 大型主机 z/OS；安全中间件和客户端/服务器应用；以及网络和通讯设备等领域。

atsec 的客户包括全球首屈一指的公司如 IBM、HP、Oracle、苹果电脑、微软、华为、银联数据、快钱、Cray、宝马、SGI、Vodafone、Swisscom、RWE 和 Wincor-Nixdorf 等。他们均选择了 atsec 作为长期的信息安全领域的合作伙伴。

浪潮SSR成为

" 中华人民共和国第十一届运动会唯一指定服务器操作系统安全加固系统产品 "



浪潮 主机安全的领导厂商

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

浪潮SSR产品系列

SSR企业版:企业核心主机操作系统免遭受非法攻击的“智能屏障”

SSR网络版:可信服务器安全运维中心

SSR专用版:为您的主机系统量身订做的“安全胃甲”

主要功能

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



inspur 浪潮

中华人民共和国第十一届运动会
IT产品与服务合作伙伴

浪潮信息安全事业部

北京办事处:北京市海淀区阜成路73号裕惠大厦1002室 邮编:100142
电话:010-68451517 (总机) 传真:68451517-6688
成都办事处:成都市一环路南一段22号红瓦大厦930 邮编:610041
电话:028-85243518 传真:028-85214223
杭州办事处:杭州文三路478号华星时代广场A楼1507 邮编:310012
电话:0571-88907770 传真:0571-88907772
南京办事处:南京市中山北路45号华美达怡华酒店7层 邮编:210008
传真:025-83308166
安徽办事处:合肥市长江中路436号金城大厦1301室 邮编:230061

广州办事处:广州市天河区北路898号信源大厦17层 邮编:510698
电话:020-38182808-8208 传真:020-38182825
上海办事处:延安西路129号华侨大厦23楼 邮编:200050
传真:021-62485588-9075
太原办事处:太原市平阳路东巷56号7号楼5单元201室 邮编:030012
济南总部:济南市山大路224号1号楼1层东厅 邮编:250013
技术支持热线:0531-85105399 0531-88932888 (总机) 转5399
售后服务热线:0531-85105398 0531-88932888 (总机) 转5398
E-mail: Security@inspur.com