



扫一扫，关注官方微信

联系我们

地址：北京市海淀区西二旗大街 39 号 A 座三 / 四层

电话：86-10-57933888

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



再次入围“央采”！亿赛通
数据安全产品线全面覆盖

刘涛航班信息遭泄露，背后的
个人隐私数据该何去何从？

"2017 信息安全与军民融合产业发展研讨会" 完美落幕



关注企业官方微信

ESAFENET Journal

中国数据安全防护专家

主办：亿赛通

策划：市场部

北京亿赛通科技发展有限公司

地址：北京市海淀区西二旗大街 39 号 A 座三 / 四层

电话：86-10-57933888

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



本刊为亿赛通企业月刊，欢迎交流，禁止转载

CONTENTS 目录

刊首语 PREFACE

2/3 刊首语

行业聚焦 INDUSTRY FOCUS

4-8 国内行业新闻

9-15 国外行业新闻

亿赛通动态 ESAFENET NEWS

16/17 "2017 信息安全与军民融合产业发展研讨会" 完美落幕

18/19 喜讯 | 再次入围“央采”！亿赛通数据安全产品线全面覆盖

20-21 亿赛通亮相 "2017 第四届国防科技工业信息安全大会"

亿赛通小贴士 ESAFENET PROMPT

22-23 黄小厨“竞标案”被曝剽窃创意？你怎么看？黄小厨“竞标案”被曝剽窃创意？你怎么看？

24-25 刘涛航班信息遭泄露，背后的个人隐私数据该何去何从？

26-27 高校学生信息泄露被放贷人骚扰：学生会给的

典型案例 TYPICAL CASES

28/29 亿赛通签约中国航天科工集团

30/31 亿赛通签约中国交通部通信信息中心

32/33 亿赛通签约中国电子科技集团公司第五十三研究所

34/35 亿赛通签约中国工程物理研究院

36/37 亿赛通签约中国兵器工业第 203 研究所



居安思危，未雨綢繆

网络时代，一个国家、一个民族的兴衰，更多地将取决于对信息这种重要战略资源的生产获取和使用的综合国力，国家之间竞争的胜利，将更多地表现为智力竞争的胜利。发达国家凭借网络技术和网络信息的垄断优势完全可能使发展中国家沦为新的“网络殖民地”，那么其意识形态安全也就无从谈起了。由此，确立并保持发展中国家网络危机意识至关重要，它有助于我们从国家政治的战略高度，清醒地认识网络发展所带来的诸多冲击，居安思危，未雨绸缪，一方面要掌握网络、运用网络，另一方面要积极寻找应对策略。习近平总书记也在十九大报告中提出“要抓紧突破网络发展的前沿技术和具备国际竞争力的关键核心技术，加快推进国产自主可控替代计划，构建安全可控的信息技术系统。”作为信息化建设的“大国重器”，中国数据安全防护专家——亿赛通，有着义不容辞的责任，11月期刊精彩呈现，带你一起回顾你身边的安全大事、小事。

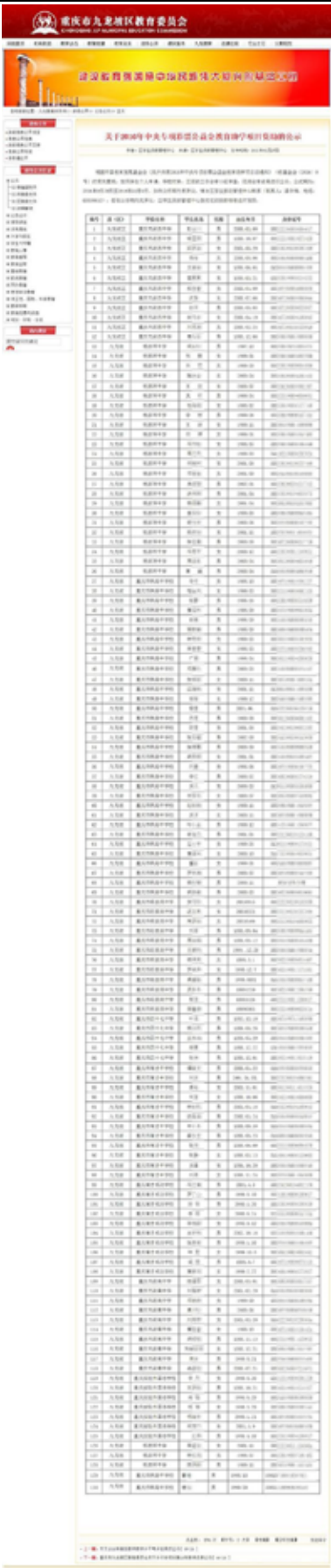
1、多地高校国家奖学金名单公示泄露隐私：含身份证号

国家奖学金获奖名单网上公示，也成了个人信息泄露的重灾区。据报道，不少高校近几年在公示国家奖学金候选人或获得者名单时，均披露了学生完整的身份证号码。有学校表示，一直以来都是这个做法；也有学校表示，给学生发奖学金，需要身份证号公示进行名单核实；还有学校表示，既要公示又要让学生核对清楚个人信息，“没有想到更好的解决办法最大限度地保护学生的隐私”。

用来奖励特别优秀学生的国家奖学金，在江苏、广西、陕西一些高校进行名单公示时出现了隐私信息泄露现象。记者注意到，河海大学、广西民族大学、西安音乐学院等高校近几年在进行国家奖学金候选人或获得者名单公示时，均披露了学生完整的公民身份证号码。

2、安徽多个乡镇社区服务中心信息泄露 目前正进行整改

11月9日，安徽铜陵市政府信息公开网、合肥市政府信息公开网等官方网站存在泄露个人信息的情况，包括姓名、联系电话、身份证号码等涉及隐私的个人信息均可从上述网站公开获取。安徽省政府办公厅发布了《安徽省人民政府办公厅关于迅速开展涉及个人隐私政府信息公开排查工作的通知》，要求全省各地、各部门网站政府信息公开平台（网）迅速开展涉及个人隐私的政府信息公开排查工作。



3、重庆九龙坡区教委官网不泄露上千教师个人信息

重庆市九龙坡区教育委员会官方网站同样存在多份文件泄露教师、学生个人信息的情况，当地相关部门迅速进行了整改。

4、为防止个人信息泄露 公安部将推行电子身份证

身份证可以说是我们生活必备，不过，身份证上信息泄露也给不少人的生活带来了麻烦。 据不完全统计，2016 年我国通过不同渠道泄露的个人信息达 65 亿条次！ ！ ！也就是说，平均每个人的个人信息至少被泄露了 5 次！ 身份信息的泄露给骗子犯罪提供了作案帮助，像徐玉玉式悲剧的发生就是因为信息泄露。 为了打击犯罪，为了更好的保护我们的信息，公安部终于放出了“大招”，电子身份证标识载入手机卡的时代即将来临！ 不法之徒的好日子即将一去不复返！



5、量子计算强“矛”将至 网络空间铸“盾”在即

随着量子计算的不断突破，其计算机能力的大幅跃升将为网络安全带来新挑战——许多加密算法将会变得相当脆弱。未来，如何应对量子计算对数据的“暴力解密”？当前移动互联网、云计算、大数据、物联网快速融合发展，对密码算法能力提出的新挑战如何应对？日前，为应对量子计算攻击威胁，移动互联网、云计算等领域数据可信融

合安全挑战，国家“网络空间安全”重点专项中唯一的密码算法项目“新型数据保护密码算法研究”项目在成都启动。由中国电子科技集团公司第三十研究所牵头的该项目，通过创新密码理论，发展新的密码技术体制，设计新型密码算法等，为我国建立新型密码算法体系，形成网络空间安全的密码核心技术。

6、政府网站公开信息中 意外涉及个人身份信息



景德镇市人社局官网上，出现一则名为“大学生一次性创业补贴人员花名册”的文件，普通用户无需登录，即可下载。而在表格中，14名创业大学生的学号、身份证号、手机号码等信息均有载录。新京报随机拨打其中4名大学生电话，均表示此前曾被告知领取创业补贴需进行公示程序，但对个人信息被一并发布一事不知情。此后景德镇市劳动就业服务管理局社区和企业服务科一名工作人员确认，文件由该单位发布并公开，其表示，姓名、学号等信息属于需要公开内容，之所以公开身份证号，是为防止因重名引起的不便。上述工作人员表示，将对文件涉泄露个人隐私一事进行处理。11月14日涉个人信息泄露的文件目前已被撤下。

7、聚焦个人信息安全：超八成 网民因信息泄露受不良影响

“当前，个人信息频繁泄露、大数据安全顶层设计缺失、大数据交易安全第三方监督缺位，在这样的背景下，出台个人信息保护法将成为保护网络信息安全的重要措施。”

8、“退改签”诈骗引出信息 泄露大案 涉多家航空公司

非法入侵 50 多家民用航空类公司网站，窃取乘客票务信息，再利用这些信息实施网络诈骗，骗取金额 1000 多万元。近日，浙江省温州市公安局网安支队、苍南县公安局网警大队破获一起特大黑客攻击窃取国内航空公司网站信息案件。警方共抓获黑客林某等犯罪嫌疑人 20 名，缴获航空票务类公民信息 30 多万条和大量账号、密码信息。



9、安全研究：谷歌揭示网络钓鱼威胁要比数据泄露严重得多

谷歌近期公布了一份长达一年的 Gmail 账户劫持调查的结果，发现网络钓鱼对用户的风险要比数据泄露的风险要大得多，因为他们收集了更多的信息。网络钓鱼的受害者比随机的谷歌用户更有可能被劫持的机率高 400 倍，而这一数字对于数据泄露的受害者来说是 10 倍。这样的数据都证明了网络钓鱼网站的威胁到底有多大。



10、追问现金贷，更需追问背后用户信息泄露

一些现金贷平台并不仅仅满足于应用上的导入口带来的收益，除了明面上的流量交易，用户数据还在暗地里被平台多次倒卖。在应用里，你若想获得较高的贷款额度，填写的资料自然是越详细越好。除了常规的电话号码、身份认证、银行卡等信息外，平台往往还会要求用户填写社保、车辆、公积金等个人信息。而这批有强烈借贷意愿的客户的资料，自然也价值连城。在羊毛党的圈子里，有一个“骗资料”的说法，就是指某些平台打着现金贷的名义骗取用户的资料，实际上并不会放款，只是通过贩卖资料赚钱。当我们在追问现金贷商业模式之时，或许更值得追问的，是其从用户获取、资金来源、风险管理等每一个环节背后的利益链条。



1、美国国防部数据库泄露 美军网络社交用户监控数据曝光



11 月 19 日三台隶属于美国国防部（简称 DoD）的错误配置 Amazon S3 服务器，其中包含来自世界各地用户的 18 亿份社交媒体与论坛发帖，不少美国民众的言论信息也包含于其中。

UpGuard 公司安全研究员克里斯·维克瑞表示，他发现三台隶属于美国国防部（简称 DoD）的错误配置 Amazon S3 服务器，其中包含来自世界各地用户的 18 亿份社交媒体与论坛发帖，不少美国民众的言论信息也包含于其中。而这批数据库分别被命名为“centcom-backup”、“centcom-archive”以及“pacom-archive”。根据名称来看，这些数据库明显属于美国中央司令部（简称 CENTCOM）与美国太平洋司令部（简称 PACOM）两大国防部下辖的军事指挥部门。

2、墨尔本国际射击俱乐部数据库被黑，超 1500 支枪械信息被泄露

墨尔本港警方在最近显得十分忙碌，但并不是忙于处理繁忙的货运事务，而是调查关于墨尔本国际射击俱乐部数据库被黑案件。有黑客在本月攻破了该俱乐部的数据库，其中包括超过 1500 支半自动手枪的信息记录，它们分属于 540 名俱乐部会员。数据具体记录了每位会员姓名、家庭住址、联系方以及拥有的枪械数量、类型和存放地点。



3、印度国家身份识别系统 Aadhaar 数据泄漏： 超 210 个中央政府网站暴露公民身份信息

据外媒 IBTimes 报道，印度执法部门 RTI 于近期发现超过 210 家政府网站在线曝光了该国 公民身份识别系统、全球最大的生物识别系统 Aadhaar 详细信息，其中包括公民姓名、地址、Aadhaar 号码、指纹与虹膜扫描及其他敏感数据。目前尚未公布数据泄露严重程度。

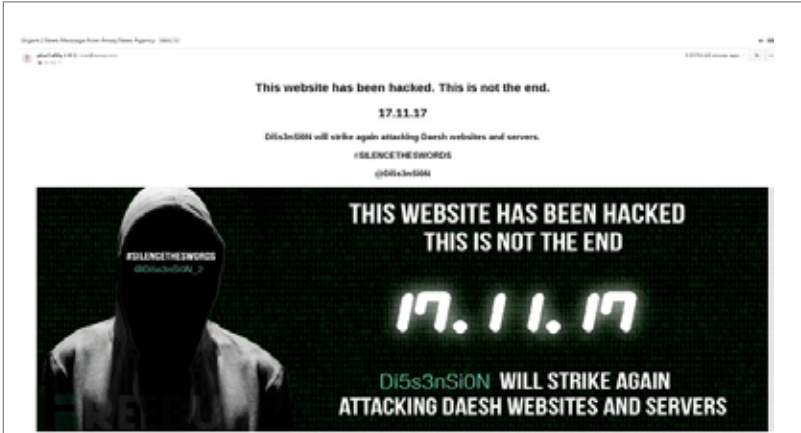


4、加密芯片漏洞或危及 近 76 万爱沙尼亚国民电子身份证安全

近期，IT 安全研究人员发现，瑞士公司 Trub AG 为爱沙尼亚国民制造的电子身份证中，所使用的加密芯片存在漏洞，或危及逾 76 万爱沙尼亚国民电子身份证安全。不过，好在该国已立即针对国民电子身份证系统进行升级。



5、穆斯林黑客攻击 ISIS 网站， 泄露 20000 用户名单

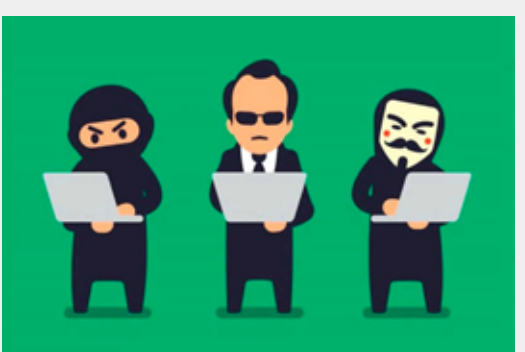


一个星期前，这个名叫 Amaq 的网站宣称，它正面临着越来越多的网络攻击。网站已经增加了安全性，现在他们的管理员可以处理“任何类型的黑客攻击”。“针对最近的事件，我们已经对我们的系统实施了更严格的安全措施。我们现在可以处理电子邮件攻击或任何类型的黑客攻击，”独立报收到的来自 ISIS 的阿拉伯语电子邮件写道。

6、美国时装品牌 Forever 21 遭黑客 入侵 致大量顾客支付卡数据泄漏

美国快时尚品牌 Forever 21 周二表示，旗下部分门店支付数据遭到未经授权的访问，今年 3 月至 10 月期间在涉及门店消费过的消费者信息或遭泄露，目前品牌正在紧急调查该事件，但暂时无法给出完整结果。Forever 21 目前在全球 57 个国家经营超过 815 家商店，品牌未透露具体哪家门店受影响。这段时间与 Louis Vuitton、AKIRA、INDEPENDENT、Levi's 联名的潮牌 Supreme 也发生了消费者数据泄露的案件。近日有消息人士称，在过去两个月中分别有三位消费者在美国的 Supreme 店铺使用信用卡消费后，存在其它国家被盗刷的经历。

然而，就这样一个颇受美国年轻人喜爱的潮服品牌，却在本周二时传出遭遇黑客攻击的消息：Forever 21 公开宣布，公司似乎陷入了支付卡数据泄露的事件。



Forever 21

7、五角大楼 AWS S3 配置错误 暴露 美国政府搜集全球 18 亿用户上网信息

据外媒 IBTimes 报道，网络安全公司 UpGuard 研究人员 Chris Vickery 于今年 9 月中旬发现美国五角大楼托管的 3 台亚马逊 AWS S3 服务器“centcom-backup”、“centcom-archive”与“pacom-archive”因配置错误，导致任何未经授权的用户均可公开访问。值得注意的是，其中一台服务器竟包含了美国国防部（DoD）从各新闻网站、评论栏、网络论坛以及 Facebook 等社交平台搜集的近 18 亿用户（绝大多数都是全球守法公民）在线发布的切身内容，且此举似乎于 8 年前就已开始（2009-2017）。

Vickery 表示，由于此次泄露的数据是情报人员通过用户公开发布的帖子整理而成，因此它仅仅暗示了美国政府有意监视的内容。尽管在线公开的数据库没有包含任何敏感信息，但美国政府确实搜集了用户社交信息，以及所发布不同内容的用户数据。此外，该数据库中的社交内容包含了多国语言，不过主要是英文、阿拉伯文与波斯文。



8、英国网络安全中心：俄罗斯企图 入侵英国国家媒体、能源及电信系统

据英国 IBTimes 报道，英国网络安全中心主管 Ciaran Marti 近期警示，俄罗斯政府疑似针对英国媒体、能源以及电信行业发动电网攻击，致使国家网络及关键基础设施面临断电危险。Marti 表示，目前俄罗斯已成功利用拒绝服务（DoS）攻击大量英国网站并企图破坏国际体系。



9、特朗普政府发布新 VEP 机制， 以防国家组织私自“库存”漏洞



据外媒 ZDNet 报道，美国白宫网络安全协调员罗伯·乔伊斯（Rob Joyce）于本周三在华盛顿特区出席活动时宣布，特朗普政府已发布一套非机密规则来更新 Vulnerabilities Equities Process（VEP）机制，以平息舆论中政府大量“库存”漏洞发起黑客攻击的虚假谣言。

VEP 是奥巴马就任时所发布的一套复杂而重要的保密机制，决定了美国政府在发现漏洞后衡量是否秘密通知受影响的科技公司，并提醒其产品或服务存在漏洞，以便黑客入侵前迅速修复。

10、新加坡完善新网络安全法 案，保障国家关键基础设施安全

新加坡于今年 7 月首次公布一份新网络安全法规草案，旨在保障国家网络安全、维护关键基础设施（CII）并授权当局履行必要职责，以促进各关键部门信息共享。据称，新加坡政府已列出 11 个被认为拥有 CII 的部门，其中包括水资源、医疗、海运、媒体、信息、能源与航空等机构。



11、英国协同办公软件存漏洞 或致英国医疗服务机构信息泄露

据英国媒体 BBC 报道，安全研究人员于近期访问毕马威会计师事务所 (KPMG) 共享的工作日志时意外发现英国协同办公软件 Huddle 存在一处安全漏洞，致使用户敏感信息在线泄露。目前，该研究人员已通过毕马威无关的签名证书获取公司财务信息。此外，英国国家卫生服务组织 NHS、内政部和税务及海关部等超过 16 万家机构均使用了该办公软件处理企业工作。



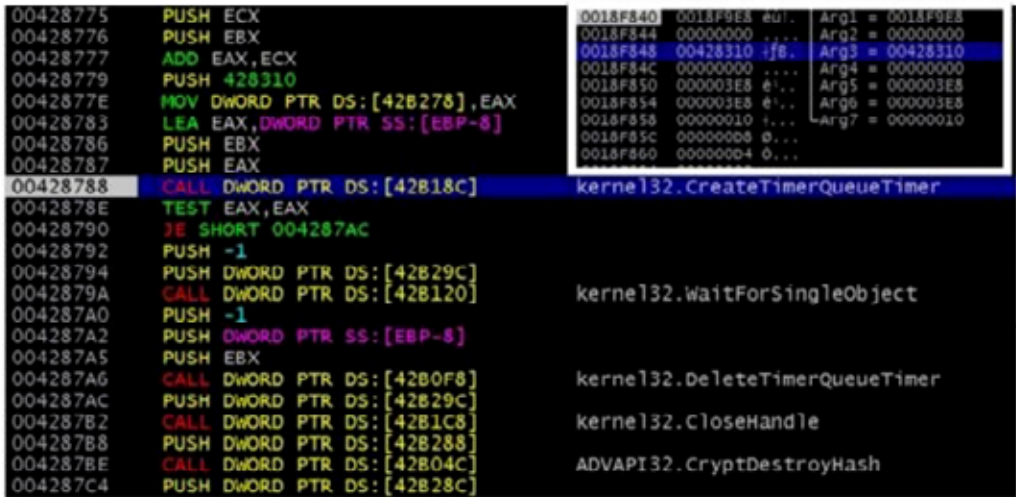
12、美国国会是如何全力推进 网络安全相关立法的



E 安全 11 月 14 日讯 面对日益严峻的网络威胁，美国国会已采取重要举措，旨在保护消费者数据泄露问题，威慑外国威胁，筹划关键机构在网络、政府信息技术采购相关事宜，确保无人驾驶车辆的安全问题等。针对这些问题的法案仍面临障碍，其中一些障碍还可能无法逾越。但美国国会围绕网络全问题采取了相关的行动。

13、银行木马 Emotet 出现新型 变种，可窃取用户金融凭证、 利用 Windows API 检测沙箱

Emotet 又名 Geodo，是目前流行的一款银行木马，首次曝光于 2014 年 6 月，其主要以 “嗅探” 网络活动窃取用户私人数据闻名。随着开发人员的不断优化，其影响规模可与 Dridex 和 Feodo 媲美。Emotet 主要通过附带恶意链接的垃圾邮件进行肆意分发，一旦用户点击触发后攻击者将通过该恶意软件窃取用户重要凭证。



"2017 信息安全与军民融合产业发展研讨会" 完美落幕



冬日里的一场盛会

2015 年 3 月 12 日，习近平在中国十二届全国人大三次会议解放军代表团全体会议上，第一次明确提出：“把军民融合发展上升为国家战略”。中共中央政治局 2017 年 1 月 22 日召开会议，决定设立中央军民融合发展委员会，由习近平任主任。

2017 年 3 月 26 日，中原军民融合产业联盟在洛阳成立，标志着以洛阳为中心、辐射中原地区的军民深度融合大格局已经形成。随着信息化建设的不断深入，信息系统

的安全性已经成为“军转民、民参军”的过程中面对的重要问题，如何防止数据泄漏？如何做到军工企业精细化、分类分级管控等合规性要求？这不仅关乎企业的命运，更关乎国家的安全。

2017 年 11 月 17 日，受中原军民融合产业联盟之委托，亿赛通联手华中大区钻石代理商洛阳沃客，成功举办“信息安全与军民融合产业发展”研讨会，汇集百余重点军工企业和信息安全、数据安全方面的专家代表，共同探讨军工信息安全发展趋势，分享信息安全创新新技术。



在国防信息化带动军工企业信息化的不断深入发展中，以及军民融合从初步融合到深度融合的过度中，我们认真听取了来自军民融合产业联盟秘书长的精彩汇报。秘书长指出：新技术、新成果、新动力，努力打造新的增长引擎，军工行业是国家军事装备重要的科研生产单位，其数据和信息安全关系到国家层面的安全和利益，军民融合全面应对新形势下的信息和数据的泄漏问题，是大势所趋，亦是发展必然。



亿赛通亮相“2017 信息安全与军民融合产业发展研讨会”分别从军民融合产业网络安全建设体系、新形势下网络安全面临的现状与挑战，并结合实战经验进行深度剖析，专业的咨询服务、完美的解决方案、经典的军工案例引爆全场。

亿赛通智能数据安全产品在满足国家安全法、保密法、网络安全法、等保 2.0 及十九大对军民融合提出的一系列法规要求下，将军工行业各类信息进行智能分类、分级，从数据采集、传输处理，到对终端层、服务层以及网络层各种形式的敏感和涉密数据进行全面监管，真正做到数据传输的有据可查，有源可溯，全方位保护内部核心数据资产不外泄。



Military information security

亿赛通为党政军行业提供，终端数据防护、网络数据防护、应用数据防护、存储数据防护、介质数据防护、云服务平台、一体化的企业综合数据安全防护体系，集 DLP 智能识别，文档分级分类、标密定密、文档智能加密，安全网关等产品的综合部署应用，通过端到端对文档全生命周期进行管理，确保数据在使用、传输和存储过程中不被未授权的用户泄露或者篡改。结合企业特有的业务需求、业务模式和管理文化，实现全方位地保护政府、军工企业数据安全。



喜讯 | 再次入围“央采”！亿赛通数据安全产品线全面覆盖



当前位置: 首页 > 中标(成交)公告

中央国家机关2017年软件协议供货采购项目中标公告

时间: 2017-10-31 10:49:00 发布: 侯少华 点击: 2997

【字体: 大 中 小】 打印预览

中央国家机关2017年软件协议供货采购项目中标公告

1、项目名称: 中央国家机关2017年软件协议供货采购项目

2、项目编号: GC-HG1170759

3、招标公告发布日期: 2017年9月5日

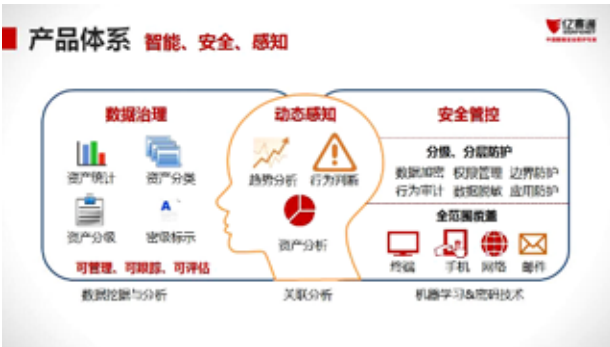
4、变更公告发布日期: 2017年9月30日

5、开标日期: 2017年10月21日

近日，中央国家机关 2017 年软件协议供货采购项目（以下简称央采）中标名单对外公示，亿赛通数据安全产品线成功入围数据泄露防护、文档加解密等产品采购项目，此次入围标志着亿赛通在继续站稳八大行业市场的同时，又一次荣获中央政府采购入场券，相信未来，在中央政府采购领域亿赛通佳绩将会再上一个新台阶。

高标准 高要求

中央国家机关集中采购项目由中央国家机关政府采购中心组织，是中国政府采购领域级别最高的采购项目之一，一直以高标准、严要求、规范化而著称，对于入围厂商的产品品牌、市场口碑、产品品质、技术含量、售后服务均设置了国家级门槛，只有各方面都展现出优秀实力的厂商才有资格入围。中央政府采购范围覆盖国务院、国务院组成部门（即中央部委等）、直属单位（如海关总署、中科院、国家林业局等）以及相关单位（如教育部直属高校等），是中国国家政务信息化建设的采购主要方式，同时也是地方政府采购的风向标。



稳扎稳打

亿赛通作为耕耘在中国数据安全防护领域 14 年的老牌企业，一直用“专注”书写着自己在安全领域的历程。截止目前服务的客户超过万家企业，终端活跃用户过百万。业内服务规模覆盖 28 个省市、4 个直辖市，开创 11 项技术专利先河，获得了 30 余项软件著作权及百项荣誉证书。

今天再次中标央采项目，充分证明政府对亿赛通在数据安全领域的高度认可。同时，在伴随着中央政府对于本土化自主研发产品的采购需求逐步加大，国产化要求越来越高，数据安全产品也被赋予了越来越多的职责，其基础和核心地位愈加凸显。相信在政府的领导下、企业的支持下，亿赛通未来之路将会越走越好。

稳扎稳打、步步为营！

亿赛通亮相 "2017 第四届国防科技工业信息安全大会 "



为进一步提升军工领域基础信息网络和重要信息系统安全保护能力，推动信息安全体系建设，促进交流合作和新一代信息安全技术应用，支撑行业发展，在国家保密局、国防科工局等相关主管部门支持与指导下，军工行业信息化高峰论坛理事会和国家科工局信息中心，于11月23日至25日在深圳举办了“2017 第四届国防科技工业信息安全大会”。亿赛通携“智能铸就安全 态势感知未来”亮相全场，成为最耀眼的一颗闪亮之星。



参会人员包括各军工集团公司、中国工程物理研究院及所属基层单位，中科院所属有关单，工信部所属高校，地方军工及民口配套单位信息化、运维、保密及相关部门负责人和业务骨干，并结合新形势下国防科技工业信息安全保密挑战与应对策略、军工智能制造与信息安全保密、军工单位工业控制系统信息安全、新一代信息技术应用安全保障、互联网安全监控体系建设及基础网络信息安全保障等一系列话题展开讨论。

亿赛通作为中国数据安全防护专家，荣幸受邀与各军工单位一起研讨军工工业信息安全的发展态势和防护需求，全面阐述了我国国防工业信息化安全防护的必要性及主要手段，并在现场直观的展示了智能数据安全的综合防御体系和解决方案，用“智能”诠释“安全”，用“智能”渲染“未来”。新时代下军工工业信息安全建设任重道远，亿赛通用它独有的企业特性、产品技能，为我国数万家军工企业提供全面周到的数据安全服务，利国利民利企业，为国防科工信息安全保障体系的建设贡献力量。



黄小厨“竞标案”被曝剽窃创意？ 你怎么看？



谁动了谁的奶酪？

曾一度沸沸扬扬的“黄小厨 noob 市集”案，如今一审宣判侵权不成立，一路的辛酸历程，谁的责任谁的问题，日后如何化解？还未尘埃落定，到底谁动了谁的奶酪？

2017 年 2 月惠恩公司（全称北京惠恩咨询有限公司）参与了黄小厨公司（全称黄小厨新厨房生活（北京）有限公司）“2017 黄小厨 noob 市集”活动策划的招投标项目，后未竞标成功。今年 4 月 22-23 日，黄小厨公司在北京朝阳颐堤港组织了该活动。



案件背景

惠恩公司指出，“2017 黄小厨 noob 市集”活动现场门头、签到处、帐篷与其竞标策划设计相同，入口处、签到区、黄小厨表情以及集印章逛市集、黄磊逛市集录直播、厨房乱打、动感单车、健康瑜伽等活动与其竞标方案相似。

认为黄小厨公司侵犯著作权，惠恩公司将黄小厨公司诉至法院，要求黄小厨公司赔偿经济损失 21.6 万余元、合理费用 8.2 万余元，并要求黄小厨公司在其官方微博、官方微信公众平台醒目位置赔礼道歉、消除影响。

黄小厨公司则认为，惠恩公司方案大量使用了黄小厨公司的自有元素以及往届市集的设计和活动形式，仅在细节上略有增删改动，不具有独创性。活动围绕中标公司提出的“家减乘厨”主题进行策划，设置“有爱”、“有味”两个子主题，与惠恩公司的投标方案无关。

最终，朝阳法院一审认定黄小厨公司不构成著作权侵权，判决驳回了惠恩公司的全部诉讼请求。

专家建议

当判断设计创意是否存在剽窃时，除了是否具有相似度以外，还需要明确“黄小厨”提出的相关要求，以及业界活动是否拥有常有方案，才能判断方案是否具有独创性或原创性。“第一，‘黄小厨’公司征集方案时，是否对活动场地布置的颜色、风格、式样有具体要求；第二，要了解业界类似活动的常有方案，是否有一些成熟的背景设计、规划方案和文案。如果‘黄小厨’公司剽窃了惠恩公司具有独创性的部分，则构成侵权。”

对于目前公关公司在设计方案的知识产权上面临“维权难”的现象，小编给予拥有自主知识产权的朋友几点建议，避免日后产权流失苦不堪言：“设计公司在投标时，就需要注意保护自身的知识产权。比如在投标时，对所提交的方案打上公司的水印；要求招标单位签署保密协议，承诺竞标方案处于保密状态，未经许可不得擅自使用或向外透露，设置方案文件打开次数，禁止拷贝粘贴、禁止未授权者阅读、禁止外传等等。”此时如果拥有一个最简单最实用的软件，管理好自己作品即可拥有主动权，定会势在必得。亿赛通数据安全卫士正是可以解决以上难题，目前该产品自今年 9 月上线之后，已满足了数千名用户对外发文件的保护需求，欢迎您的关注与试用。

<http://www.2c.esafenet.com>。

刘涛航班信息遭泄露，背后的个人隐私数据该何去何从？



10月30日，刘涛发布微博，吐槽自己的隐私遭泄露，同时呼吁有关部门管管。

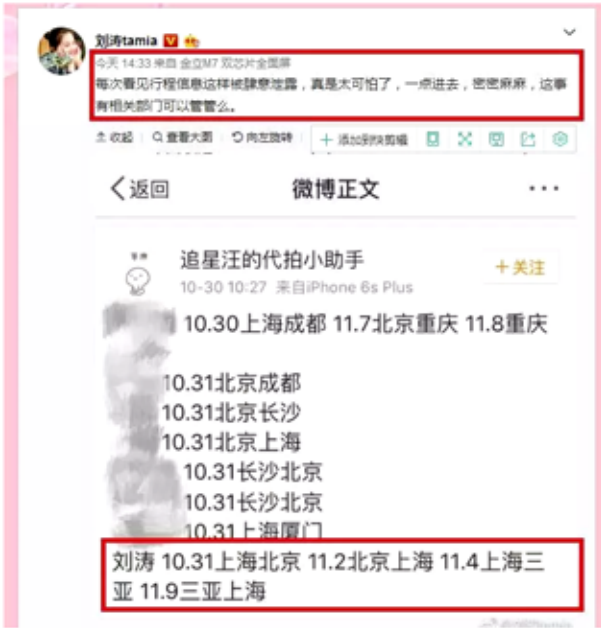
微博内容：“每次看见行程信息这样被肆意泄露，真是太可怕了，一点进去，密密麻麻，这事有相关部门可以管管么。”

刘涛在微博中配发了一张11月9日前的行程被泄露的截图。

图中有刘涛10月30日，11月2日，11月4日和11月9日的日程。

泄漏途径应该是航空部门。

对于此类隐私的泄漏，人们往往无可奈何。



@ 投我以六桃：泄露行程的真的非常讨厌了 心疼涛姐姐 [抱抱] [抱抱]

@ 欧文克拉口红抢不到_好气：那些私生饭真是够够了，明星就不能有自己的生活自由吗 [吃瓜]

@ 老铁是你小姐姐：真的好恶心！这些人都应该抓起来！



信息泄露无时无刻发生在我们身边，修个电脑数据泄露了、上传到第三方平台的照片也被扒出来，难道“艳照门”事件的警惕还不够吗？答应我看完一段段泄密小故事，相信你会回来转的~~~~

我的照片——想看！要先问问主人的意见

我的摄影作品——想卖！要先问问主人的意见

我的电脑资料——想盗！要先看看主人是谁

保护个人隐私数据，从我做起，斩断根源，防范于未然。

自从有了这个，你的隐私数据，你做主！

<http://www.2c.esafenet.com>

第一步：关注亿赛通官方微信；

第二步：回复关键词“激活码”，即可免费领取一年的会员激活码。

高校学生信息泄露被放贷人骚扰： 学生会给的

11月1日，有多名成都工业学院学生反映，在微信上收到同一放贷人添加好友的请求。对方自称是正规放贷公司，可以清晰说出学生的姓名、年级、专业及父母电话，并声称信息来源为成都工业学院学生会。

北京青年报记者通过网友提供的图片看到，该放贷人微信昵称为“缺钱找我”，通过搜索手机号添加学生微信，自称公司位于时代数码广场，并表示只要学生征信没问题、贷款不逾期，贷款利息跟银行一样，最多可以贷款几十万。

该贷款在与学生聊天中声称学生的信息来源为成都工业学院学生会，并给学生发送一张包含大量学生个人详细信息的 excel 表格。遇到此情况的学生怀疑自己的信息遭到了泄露。

对此，成都工业学院分管校学生处的团委回应称，放贷人自称从学生会获得学生信息的情况不属实，学生会从未向任何院系、班级收取过学生详细信息，也不可能对外泄露学生信息。“多数收到添加好友请求的学生都没有通过，也没有学生因此贷款或被骗。我们平时就



通过多种渠道提醒学生不要通过网贷、校园贷贷款。”

成都工业学院团委工作人员称，今天收到学生反映后，由于目前没有学生因此受害，学生不愿报警，但学校保卫部门已经介入，学生信息泄露的具体渠道还在调查中。

希望早日能够查清事实真相，也希望相关部门多一份社会责任感，如果他们早一点采取信息安全保护措施、早一点使用安全加密产品，就不会酿成今天的结局，少投入大盈利。所以，无论企业或个人一定要意识到数据安全保护的重要性，提早采取防护措施。未雨绸缪，防患未然。

亿赛通签约中国航天科工集团



客户简介

中国航天科工集团公司（简称“航天科工”）成立于 1999 年，是中央直接管理的国有特大型高科技企业。航天科工现由总部、6 个研究院、1 个科研生产基地、13 个公司制、股份制企业构成。控股 7 家上市公司。拥有多个国家重点实验室、技术创新中心、成果孵化中心以及专业门类配套齐全的科研生产体系。

需求背景

航天科工从事着关系国家安全的战略性产业，信息安全直接影响着国防安全，特别是航空信息安全问题和信息安全管理体的建立已逐渐成为国防建设的基础之一。同时，信息安全管理水平也是衡量一个航空科技现代化程度和综合实力的重要标志。因此，针对当前信息安全隐患问题，中航科工的信息泄密问题防护工作显得更必要和迫切，尤其为了防止文档存储的重要信息被窃取，必须加强文档安全管理。

方案概述

亿赛通文档密级管理系统以实现人员密级、数据密级的安全分级管理控制，满足组织数据分级安全管理要求。

项目成果

亿赛通文档密级管理系统对航天科工的核心电子文档进行细分化的权限设置，确定机密信息在特定授权范围内合法操作，保障了航天科工文档涉密信息的安全，并且为用户提供安全授权下的机密信息共享机制，实现了机密信息分权限的内部安全共享。

亿赛通签约中国交通部 通信信息中心



客户简介

中国交通通信信息中心（CTTIC），是交通运输部直属事业单位，受部委托拟订并组织实施交通运输行业通信、导航、无线电和信息化管理的技术政策、技术标准、规章制度；代表国家参与国际电信联盟（ITU）、国际海事组织（IMO）的有关活动，负责中国国际海事卫星、国际搜救卫星系统的建设、运维和管理工作，并承担国内外相关应急安全公益性通信职责，是管理国家关键基础设施的单位。

需求背景

交通运输行业作为国家的关键基础设施，在信息化融入到全球社会化迅速发展的时代，交通运输行业信息安全备受我国重视。目前国内交通运输行业信息系统复杂多样，信息安全攻击与威胁严峻、安全漏洞与脆弱性隐蔽性强，安全风险聚集、扩散性并存，构成行业信息安全风险态势严峻。因此，中国交通通信信息中心需要有效的加强中国交通通信信息的数据安全。

解决方案

- 文档透明加密系统是亿赛通文档安全管理系统的核心组件之一。
- 1、，采用第四代 VFS 技术，实现对任意文档自动透明加密。不改变和影响用户使用系统和工作效率；
 - 2、智能半透明加密，可实现对本地文档不影响工作情况下，无障碍使用密文文档，对本地敏感文档可手动加密；
 - 3、多密钥隔离管理，可实现部门动态加密文档相互隔离禁止交叉打开，管理人员可以打开各部门文档，自身文档可自动或半自动透明加密，密钥可以独立或与某个部门相同；

4、内容安全防护，防止核心数据通过复制、拖拽、截屏录制、打印输出、副本另存等方式泄密。

项目成果

亿赛通文档透明加密系统通过对中国交通通信信息中心工作者所存储的文档进行加密，层层防护，有效的保护了其内部重要信息的安全，并促进了中国交通通信信息中心的信息管理更加智能化、有序化，着实创造了一个安全办公的环境。

亿赛通签约中国电子科技集团公司第五十三研究所



客户简介

中国电子科技集团公司第五十三研究所（简称“五十三所”）成立于 1980 年，是从事光电系统总体技术研究、产品研制与生产的国家一类研究所、专业总体单位、国家级重点实验室依托单位。五十三所在我国光电工程基础研究和应用领域已形成领先优势，共取得科研成果 700 余项，其中国家级 3 项、省部级 120 余项，拥有专利 100 余项。具有国家一级保密资质、职业健康安全环境管理体系认证资质、GJB/Z9001 质量体系认证等资格及体系认证。

需求背景

五十三所作为国家光电行业重要的研发单位，对于本单位的数据信息安全问题非常重视。针对五十三所信息安全管理所存在的问题，即员工与员工之间的涉密文件相对隔离，如何进行二次开发？员工间的涉密文件需要领导审批时，流转过程中的信息安全，二次开发如何保障？以及领导层如何看到几个关联部门的涉密文件？如何管理和有序操作大量的涉密文件和网页内容存在的敏感信息？为确保各个环节的信息安全，以及提高单位信息安全防御能力，五十三所牵手亿赛通，共创数据安全运行的办公环境。

解决方案

亿赛通文档安全管理系统是一款电子文档安全防护软件。

- 1、智能透明加密：**采用第四代 VFS 技术，使用智能动态加密对经过的文档数据进行自动透明加解密，在用户没有任何感知的情况下保护文件的安全；
- 2、智能半透明加密：**可实现对本地文档不影响情况下，无障碍使用密文文档，对本地敏感文档可手动加密；

- 3、安全分级控制：**实现人员密级、数据密级的安全分级管理控制，满足组织数据分级安全管理要求；
- 4、详尽日志审计：**对所有加密文档的使用过程、各项流程审核及管理变更的相关信息进行详尽日志审计，并对审计日志提供查询、导出、备份等支持；
- 5、详尽日志分析：**详尽记录了登录日志，同时，日志收集过来，进行集中审计，便于泄密事件发生后的分析和追查。所有用户（包括管理员在内）的任何操作，系统将自动监控、跟踪并进行记录。另外，通过日志审计功能，管理员可以随时查看系统运行情况，能够及时发现一些异常操作，从根本上降低数据泄漏风险。

项目成果

亿赛通文档安全管理系统解决了五十三所数据信息的安全隐患问题。保障了数据传输的安全，以及员工涉密文件的信息安全。同时，提高了五十三所整体的信息化水平和工作效率和员工的信息安全保密意识，促使了单位信息管理有序，打造一个良好的信息安全办公环境。

亿赛通签约中国工程物理研究院



客户简介

中国工程物理研究院（简称“中物院”）成立于 1958 年，是国家计划单列的我国唯一的核武器研制生产单位。院内云集了一大批国内顶尖科学家，并设有科研机构、技术保障等单位，主要从事冲击波与爆轰物理、核物理等离子体与激光技术、工程与材料科学、电子学与光电子学、化学与化工、计算机与计算数学等以发展国防尖端科学技术为主的集理论、实验、设计、生产为一体的综合性研究院。

需求背景

鉴于中物院计算机信息系统的应用越来越普及，面临的信息安全形势越来越严峻，如国防尖端核心数据泄露、互联终端遭非法操控、甚至发生黑客通过入侵国防尖端科技网络系统攻击国家研发的核心技术的事件等，因此有必要对院级面临的信息安全隐患进行梳理，解决和提升国防领域信息安全的保障能力。

解决方案

亿赛通数据泄露防护（DLP）系统是一款基于内容识别技术，主要解决发现、识别、分类企业敏感数据；监控企业敏感数据使用情况；保护企业敏感数据以防丢失和被窃；防止敏感数据通过打印、刻录、聊天工具、发送邮件等方式泄露出去，严格管控文档在使用中的各种安全隐患问题。

项目成果

亿赛通数据泄露防护（DLP）系统提供了对中物院内网综合一体化防护，提升了等级管理建设能力，以及实现了敏感数据可保护，安全态势可度量，安全事件可追溯，完成了中物院信息安全的整体布局建设需求，从而保障了信息系统中所有数据的全生命周期安全。

亿赛通签约中国兵器工业第 203 研究所



客户简介

中国兵器工业第 203 研究所始建于 1956 年，是从事国防技术研究的大型综合性研究所。建所 50 多年来，一直承担着国家重点科研任务，成果斐然。在党中央、国务院、中央军委和各级地方政府、集团公司的关怀和领导下，共获科技成果奖励 1500 余项，其中国家级科技成果奖 30 余项，省部级科技成果奖 120 余项，是国家技术改造的重点投资单位之一。

需求背景

目前针对军工涉密数据的保护手段大多采用专用涉密网络进行内外网物理隔离和三合一保密软件进行移动存储介质管理的方式，但数据本身还是以明文方式存在。鉴于目前复杂的业务应用场景和无处不在的数据，传统的以封堵终端和外部处理设备的安全保护方式已经无法满足军工高敏感数据的保护要求。在涉密数据的使用、传输、保管的过程中仍存在较多安全隐患，数据泄露风险。因此中国兵器工业第 203 研究所有待加强终端文档安全。

解决方案

亿赛通终端数据防护系统主要为防止非法获取应用系统数据的安全防护系统；

- 1、统一身份认证：**完善的统一用户身份认证管理体系，支持 LDAP 和 OPENLDAP 的集成。
- 2、数据安全传输：**数据始终以密文形式传输、存储和使用，保障传输过程中的安全。
- 3、终端数据加密：**移动终端采用底层动态加解密核心技术，保障落地数据安全。

4、终端自我保护：全球首创底层 Anti-hacking 技术，防止移动终端应用程序被反编译或破解。

项目成果

中国兵器工业第 203 研究所通过对终端文档安全管理系统部署，涉密数据安全保护体系以数据加密为核心，以涉密数据的安全技术管控保障为落实关键，结合单位业务发展规划及保密条例与等保合规要求，构建完善了单位涉密数据安全保护体系。