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 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　中国数据安全防护专家　www.esafenet.com

4 月刊

2019 年共 11 期

关注企业官方微信

Esafenet
Monthly magazines

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责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS目录

刊首语 PREFACE

大数据时代，《亿赛通四月刊》直击信息安全痛点

习总书记曾指出，要构建集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体的国家安全体系。

近年来，随着网络诈骗的日益增多，信息安全问题变得愈发突出，构建国家安全体系需要大力维护好信息安全。信息安全是信息技术双刃剑效应的集中体现。一方面，信息技术越发达，个人信息暴露的可能性就越大，程度也越深。从文字、图片到音频、视频，在信息技术节节攀升的同时，个人信息保护也越来越无险可守，越来越轻易就能被用来在更加广袤的时间和空间中传播。另一方面，信息技术的发达，让一些远程、非现场的犯罪更加复杂、隐蔽、多样化，令人防不胜防……

国内

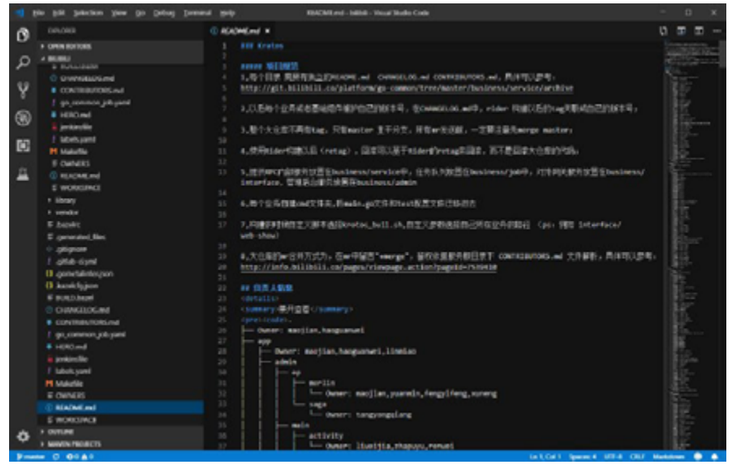
1、女子购物信息泄露 被假客服设套骗走 5 万余元

摘要：4 月 16 日，黄女士接到一个云南的电话，一名女子自称是京东商城客服人员。对方称她购买的奶粉出现问题需要退款，一步步设下陷阱，最终骗走 5 万元。

2、四万多条小区业主信息这样被泄露

摘要：近日，香洲区法院审结一宗侵犯公民个人信息的案件，男子罗某向某地产公司门店经理余某出售 4 万多条小区业主个人信息资料，构成侵犯公民个人信息罪，罗某、余某以及曾某 3 名被告人被判处有期徒刑一年八个月至十个月不等。

3、网曝 B 站整个网站后台工程源码泄露



摘要：近日，有消息称 B 站整个网站后台工程源码泄露，这是国内规模较大的互联网企业中首例整个网站后台工程源码泄露。消息称，在该工程源码中，包括不少用户名密码被硬编码在代码里面，谁都可以用。目前 Github 已经封禁该页面。

4、联通一外包公司被指泄露数万名客户信息

摘要：4 月 11 日，河南周口联通公司“呼叫业务”外包商员工称，外包公司利用联通的客户信息推销贷款业务。外包商称不做这种勾当；联通营业厅称可当面谈，拒绝电话解释。

5、东莞通报医院候诊区播放不雅视频：初步分析系设备被入侵控制

摘要：4 月 11 日中午，长安医院一处于待机状态的智能电视机自动播放不雅视频。事件发生后，长安医院第一时间向公安机关报案，长安警方已介入调查。长安镇组织工作组到长安医院指导调查工作，并要求长安医院全面做好隐患排查工作，堵塞网络安全漏洞，保障医院网络安全。

6、她坐在奔驰车盖上哭泣，她的手机号还被泄露

摘要：4 月 15 日，奔驰车维权事件出现后续报道，西安女车主表示，舆论发酵后，网上有人说她是演员，是间谍，有人通过朋友亲人找到她，她的手机号被泄露出去，短信微信全都是陌生人的信息，甚至还有恐吓。

行业聚焦 INDUSTRY FOCUS

7、小区莫名被注册数百公司 谁让业主信息裸奔？

摘要：据报道，北京房山区长阳某小区多名业主近日发现，自家地址在不知情的情况下被人注册了公司，仅该小区的 9 号院就被注册了 599 家公司。

8、老人社保信息遭泄露，投诉三大保险公司侵犯隐私，公司：正在开会

摘要：近日，河北省马先生在微信中找到了被多次浏览和转发的一条朋友圈，上面有其父亲的住院信息和社保信息，并且病情和治疗详情被随意夸大，他知道父亲的个人信息被泄露了。

9、湖北一公职人员泄露公民信息 5 万余条，非法获利 23 万余元

摘要：近日，荆门京山市检察院依法以涉嫌侵犯公民个人信息罪对犯罪嫌疑人张某批准逮捕。张某原本就职于某工商局，2017 年 4 月以来，为谋取非法利益，利用职务便利在大数据分析平台上查询并下载了大量企业登记的公民个人信息，包括企业名称、法人代表姓名、电话号码等，后通过在网上 QQ 聊天寻找购买工商登记注册信息的“买家”，并通过 QQ 将企业登记的公民个人信息发送给客户。经公安机关鉴定，其提取、下载公民个人信息 5 万余条，获取非法利益 23 万余元。

10、说好的不泄露呢？中介可从安居客后台获得用户个人隐私

安居客

摘要：近日，苏州的赵先生反映，他在线上租房平台“安居客”应用上浏览二手房信息，并且使用该软件自动生成的虚拟号码向当地一家中介公司进行咨询。可电话刚挂不久，中介公司方面就掌握了赵先生的真实电话号码。调查发现，中介公司能从“安居客”网站后台获得用户个人号码信息。

11、云集被质疑泄露个人信息，千名消费者惨遭电话诈骗

摘要：多名消费者反映，在云集平台上购物之后接到了诈骗电话，导致上当受骗。北京市消费者时小姐在云集 APP 上购买了日本 pitta mask 口罩，结果当天晚上就遭受了诈骗，被骗子分 19 笔划走了 14000 元。山东青岛消费者谢小姐在云集 APP 下单购买了女性日常用品，骗子能报出她的单号和购买的物品，谢小姐被骗 4999 元。

12、绍兴 10 余万条学生家长信息遭泄露

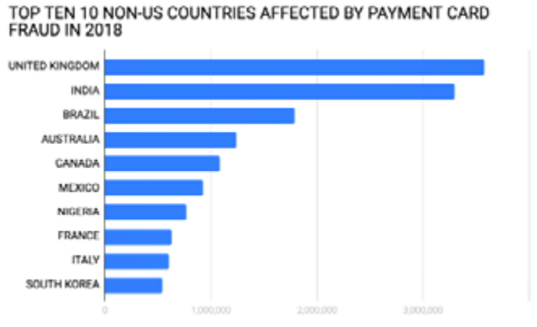
摘要：近日，绍兴市公安局越城区分局破获了一起案件，10 余万条学生家长的信息遭到了倒卖。绍兴市民向公安局反映老是接到培训机构的推销电话，但自己从来没有去过，也没留过联系方式。调查后发现，这些居民的孩子都是小学、初中的学生，推销电话的源头是越城区、柯桥（区）的两家教育培训学校。警方从他们培训机构的 U 盘里面发现了学生个人信息。这是一份完整的 2015 年全市中小学学籍数据，信息多达十余万条，内容包括学生、家长的姓名、联系方式、家庭住址、学校班级信息等。

国外

1、Oracle WebLogic 服务器高危安全漏洞预警

摘要：2019 年 04 月 17 日，360CERT 检测到 Oracle 于 4 月 17 日发布的安全公告。该安全公告披露 WebLogic 服务器存在多个高危漏洞，影响到多个 WebLogic 组件。360CERT 判断此次安全更新针对的漏洞影响范围广泛，黑客利用漏洞可能可以远程获取 WebLogic 服务器权限。

2、印度支付卡欺诈发案率快速上升 名列全球第二位

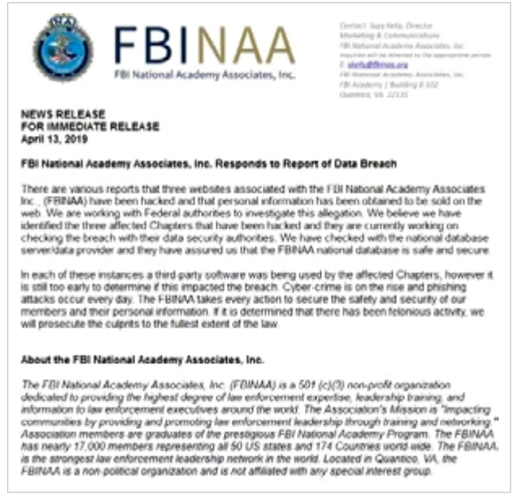


摘要：根据某网络安全公司发布的网络犯罪统计数据，2018 年，超过 320 万张印度支付卡记录被泄露，并在网上发布供出售，这与去年相比有了很大的飞跃，当时只有 80 万张印度支付卡的详细信息被发布在网络犯罪论坛上。

3、搜 WiFi 热点 Android 应用数据泄露: 涉 200 多万 WiFi 密码

摘要：据美国科技网站 TechCrunch 报道，一款流行的 Android 热点（WiFi）搜寻 App“WiFi Finder”暴露了 200 多万个网络的 WiFi 密码。目前已有数千人下载了这款 WiFi Finder 应用，它允许用户搜索附近的 WiFi 网络。但同时，这款应用也允许用户将 WiFi 密码从自己的设备上传到数据库，供其他人使用。

4、多个美国政府网站遭遇黑客入侵 当局已展开调查


FBINAA
FBI National Academy Associates, Inc.

NEWS RELEASE
FOR IMMEDIATE RELEASE
April 13, 2019

FBI National Academy Associates, Inc. Responds to Report of Data Breach

There are various reports that three websites associated with the FBI National Academy Associates Inc., (FBINAA) have been hacked and that personal information has been obtained to be sold on the web. We are working with Federal authorities to investigate this allegation. We believe we have identified the three affected Chapters that have been hacked and they are currently working on checking the breach with their data security authorities. We have checked with the national database server/data provider and they have assured us that the FBINAA national database is safe and secure.

In each of these instances a third party software was being used by the affected Chapters, however it is still too early to determine if this impacted the breach. Cyber-crime is on the rise and phishing attacks occur every day. The FBINAA takes every action to secure the safety and security of our members and their personal information. If it is determined that there has been felonious activity, we will prosecute the culprits to the fullest extent of the law.

About the FBI National Academy Associates, Inc.

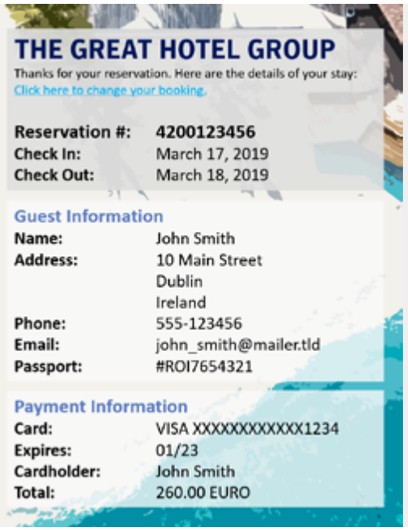
The FBI National Academy Associates, Inc. (FBINAA) is a 501 (c)(3) non-profit organization dedicated to providing the highest degree of law enforcement expertise, leadership training, and information to law enforcement executives around the world. The Association's Mission is "Impacting communities by providing and promoting law enforcement leadership through training and networking." Association members are graduates of the prestigious FBI National Academy Program. The FBINAA has nearly 17,000 members representing all 50 US states and 174 Countries world wide. The FBINAA, is the strongest law enforcement leadership network in the world. Located in Quantico, VA, the FBINAA is a non-political organization and is not affiliated with any special interest group.

摘要：日前，多个美国政府网站遭受黑客入侵，并出现数千名联邦特工及警察等个人信息遭遇泄露的事件。目前，美国当局正对此事展开调查。报道称，黑客至少入侵了三个美国政府网站，并最少泄露了 1400 份美国联邦调查局、特勤局、国会警察局、美国国家公园警察局和其他联邦机构，以及北卡罗来纳州和佛罗里达州地方警察部门的执法人员和工作人员的个人信息。据悉，泄露的内容包括当事人的姓名、住址、电话号码、个人及政府邮件地址等，这些信息在 4 月 11 日在网上发布。

5、Outlook 邮件系统爆严重漏洞 用户的邮件内容可被黑客访问

摘要：据报道，最近披露的微软 outlook 电子邮件平台漏洞比最初想象的要严重的多，目前已经影响了大量的 Outlook、MSN 和 Hotmail 电子邮件帐户，黑客能够通过该漏洞访问用户电子邮件内容。黑客未经授权访问电子邮件帐户相关信息 - 包括电子邮件地址，文件夹名称，电子邮件主题行和收件人电子邮件地址。

6、67% 酒店在无意中泄露个人信息， 第三方服务商可以替你取消订单



摘要：近日赛门铁克测试了 54 个国家的 1500 多个酒店，发现三分之二都在泄露包括客人姓名、手机、邮箱、护照号码在内的订单信息。研究员根据自己喜欢的度假地点，选择了搜索结果中排名最高的酒店进行测试，他发现，这些酒店中有三分之二都在无意中将预订代码泄露给了第三方服务商，比如广告商和分析公司，但他们的隐私政策并未明确提到这种行为。也就是说，这些第三方服务商不仅可以直接登录客人的订单，看到客人的个人信息，甚至还可以替客人取消订单。

7、未受保护的服务器公开了 1250 万女性的详细信息

摘要：由印度政府医疗机构管理的一个配置错误的 MongoDB 数据库在没有密码的情况下保持在线，暴露了超过 1250 万份孕妇病历。安全研究员确认并向印度计算机应急响应小组（CERT）报告数据泄露事件后，此事件曝光，该小组立即将服务器关闭。

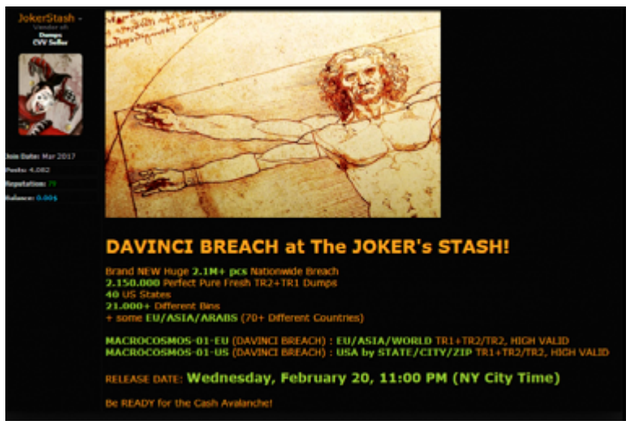
8、日本 Hoya 公司遭受网络攻击， 计算机被用于挖掘加密货币

摘要：日本光学产品制造商 Hoya 公司在 2 月底遭受了一次严重的网络攻击， 100 多台电脑感染了病毒，导致 Hoya 公司的用户 ID 和密码被黑客窃取。黑客还在攻击期间试图挖掘加密货币，工厂生产线因此停止了三天。受影响的工厂都位于泰国，不过有关攻击的详细信息尚未公布。Hoya 目前还没有完全恢复正常运营。

9、沙特政府黑入亚马逊 CEO 贝索斯手机，从中获取个人数据

摘要：据 CNBC 报道，安全主管加文·德贝克尔（Gavin De Becker）在周六表示，沙特政府黑入了亚马逊首席执行官杰夫·贝索斯（Jeff Bezos）的手机并获取到了个人数据。

10、Earl Enterprise 餐馆系统遭黑客入侵，200 多万张信用卡资料遭窃取

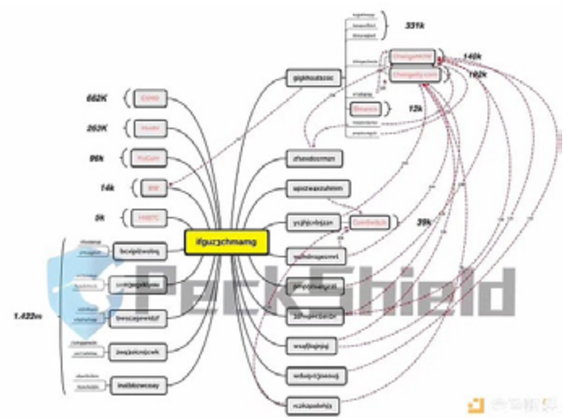


摘要：安全研究人员发现 Earl Enterprise 公司客户的 200 多万张信用卡资料遭窃取，黑客在网上叫卖窃取的信用卡信息。黑客使用“在其销售点系统上安装的恶意软件”从 210 个州的餐馆位置窃取了 215 万个信用卡和借记卡号码，到期日期以及一些持卡人姓名。

11、丰田五周内遭两次网络攻击，310 万日本车主信息泄露

摘要：据外媒报道，日本汽车制造商丰田宣布了第二次数据泄露，这是该公司在过去五周内发生的第二次网络安全事件。第一起事件发生在澳大利亚子公司，但此次受攻击的地点是在日本的几家分公司。黑客入侵了公司的 IT 系统，并访问了几家销售子公司的数据。丰田表示，黑客入侵的服务器存储了多达 310 万客户的销售信息，丰田和雷克萨斯车主的数据面临风险。

12、韩国 Bithumb 交易所私钥被盗 损失近 9 千万元



摘要：Twitter 上有消息称 XRP 地址（rLaHMvsPnPbiNQSjAgY8Tf8953jxQo4vnu）被盗 20,000,000 枚 XRP（价值 $6,000,000），通过慢雾安全团队的进一步分析，疑似攻击者地址（rBKRigtRR2N3dQH9cvWpJ44sTtkHiLcxz1）新建并激活，此后开始持续 50 分钟的“盗币”行为。根据慢雾威胁情报系统警报，韩国交易所 Bithumb EOS 冷钱包 g4yd*hege 疑似被黑，该钱包在凌晨 4 点更新了 active、owner 私钥，然后转出三百多万 EOS（（价值约 8925 万人民币））至 ifgu*mamg，且攻击者持续洗币。

2019 年亿赛通华东区渠道大会
力促伙伴同舟共济，同心共赢

大数据时代，数据安全市场需求愈加强烈。在这样的环境中，企事业单位该如何选择数据安全厂商来保障企业内部的数据资产安全？而数据安全厂商又该如何保持自我为客户提供优质的服务？

2019 年 4 月 25 日 -26 日，以“安全源自专业·信心出自底蕴”为主题的 2019 年亿赛通华东区渠道大会在苏州召开。亿赛通专家与华东地区渠道合作伙伴相聚一堂，共同探讨数据安全市场新动态，规划未来的发展方向。

顺应趋势 发展创新

会中，亿赛通专业人员分享到：目前，客户对于数据安全的需求不断提高，近年来，政府的高度重视和政策扶持也在不断推动信息安全产业的快速发展。而作为中国数据安全防护专家，亿赛通的渠道建设、产品、服务等各个环节均随着时代的发展和需求不断升级改进，只为更好的满足现实市场的需求。公司借助多年积累下来的资源与口碑，为渠道合作伙伴提供优质产品、完善政策、售后保障和多维度协作，以期合作伙伴提供更具有竞争力的销售助力和更大的市场份额。

凭借着对“持续创新”理念的坚持，亿赛通产品始终自主研发，会议现场公司专业人员从产品规划、产品方向、整体解决方案等视角向在座同仁传递前沿技术，共同探讨创新的、极具竞争力的行业解决方案，从而为最终用户创造更多价值。近年来公司在制造业、金融、能源、党政军、集团企业、研发通讯、运营商等七大行业实现了自我超越和全面突破，市场占有率遥遥领先。与此同时，亿赛通服务水平全面提升，赢得了良好的客户口碑，为市场拓展打下了坚实基础。

现场签约 严格认证

大会现场，亿赛通特举办渠道签约仪式及优秀渠道表彰环节，从此以后，公司与渠道伙伴在市场商机、产品服务等多领域，展开深度合作，双方合作再跃一个新台阶。

为促进合作伙伴的发展，适应市场需求，亿赛通专家为现场的渠道商进行详细的产品、服务综合，技术支持培训，在会议结束前进行了专业的认证考试。同时就华东区域项目工作中遇到的各种问题，大家现场展开交流沟通，进行经验分享、全面分析、深入研究、充分吸收，推动日后各项目工作取得新成效。面对客户，亿赛通严格要求每一个团队人员，始终以优质的服务标准为原则。

如今，随着公司的不断发展和业务壮大，渠道建设也开启了全新征程，未来将不断提升服务质量，全力构建渠道体系，极大限度的满足渠道伙伴们的需求，在共享全国资源的基础上，为渠道伙伴提供更广阔的发展平台。2019 年亿赛通所有伙伴都撸起袖子加油干，以坐稳中国数据安全专家的品牌之位，保障每一个企业的数据安全成为奋斗的目标！

热烈祝贺亿赛通再次通过军采平台权威认证

日前，北京亿赛通科技发展有限责任公司在经过专家组严格审核后，再次顺利通过国防科工局信息中心军民融合信息安防集采平台（以下简称“军采平台”）供应商资质认证。

入库企业审核十分严格，在公司资质、产品、服务等各方面的要求极为严苛，被成功纳入标志着亿赛通优秀的产品技术和服务能力赢得国家国防科技工业局信息中心的高度认可。

关于军采平台

军工网信综合服务平台由国防科工局信息中心军工网信综合服务平台运营办公室负责建设运营管理，接受国防科工局信息中心对平台建设的指导、考核和监督。平台为积极响应国家军民融合深度发展战略，致力于为地方政府、军工单位及民口企业供需各方和其他参与者在网络安全和信息化应用等军民融合领域提供综合服务。助力军工单位开拓军转民市场，积极引导优势民口企业融入军工体系。

军采平台主要职责是实施国防科技工业系统信息安防的集中采购，是国防科工局信息中心唯一指定的军工系统内信息安防领域集中采购平台。无缝对接国家级企业诚信档案信息库，建立适用于军工系统的诚信管理体系，全面服务国防科技工业系统信息安防的集中采购，是“军转民、民参军”信息安防产品采购需求信息的权威发布及军工系统招标采购的重要服务平台。

技术奠定实力

作为当前数据安全行业的佼佼者，亿赛通坚持自主创新，致力于文档加密、数据库审计、勒索病毒防护等技术在数据安全领域中的应用与探索。多年来，企业用实力证明了自身的产品研发水平与市场拓展能力，用户群体在高速扩增，越来越多的政府机关、军工机构选择亿赛通保障自身数据安全。未来亿赛通将保持创新精神，研发更安全的行业解决方案，为党政军行业及更多的企业用户打造全方位的安全防护产品，建立起畅通、互信、共赢的合作桥梁，保障用户生产及办公环境的安全，为用户的网络安全和数据安全不懈努力。

亿赛通双项产品喜获“北京市新技术新产品（服务）证书”

近日，北京市科委等六家单位联合发布了“第九批北京市新技术新产品 (服务)”认证名单公示。北京亿赛通科技发展有限责任公司自主研发的“电子文档安全管理系统（CDG）”及“数据泄露防护（DLP）系统”两款技术产品皆成功入选。

据了解，“北京市新技术新产品（服务）认证”旨在推动高新技术产业的发展，为企业创新和科研能力的提高注入动力，具有极高的权威性。作为北京市新技术新产品，应具有技术先进性和创新性，并拥有自主知识产权，技术成熟、质量可靠。经认定后的新技术新产品（服务），可享受政府采购和推广应用等政策支持。本次“电子文档安全管理系统 (CDG)”、“数据泄露防护（DLP）系统”产品证书的获得是对企业产品技术创新性和市场前景的肯定，进一步体现了也彰显了亿赛通的市场竞争力。

电子文档安全管理系统（CDG）

电子文档安全管理系统（简称：CDG）是一款电子文档安全防护软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产，对电子文档进行全生命周期防护，系统具有透明加密、主动加密、智能加密等多种加密方式，用户可根据部门涉密程度的不同（如核心部门和普通部门），部署力度轻重不一的梯度式文档加密防护，实现技术、管理、审计进行有机的结合，在内部构建起立体化的整体信息防泄露体系，使得成本、效率和安全三者达到最优平衡，实现电子文档的数据安全。

数据泄露防护（DLP）系统

数据泄露防护系统是基于内容识别技术，对设计图纸、源代码、合同文本、财务报表等敏感文件进行数据安全保护，防止通过邮件、聊天工具、网盘、U 盘拷贝、打印等途径泄露数据，对用户泄密行为进行记录、告警、阻断，并对用户行为进行审计。有效识别敏感数据，监控敏感数据使用情况，防护敏感数据外泄。有效培养并提高员工对敏感文件的保密意识。

亿赛通始终把技术创新作为企业发展的核心驱动力，坚持开发新技术，研制新产品，不断完善改进产品功能，使产品始终处于行业前列。证书的颁发亦是对亿赛通在数据安全领域技术和产品服务实力的充分肯定。未来，企业将继续在研发路上潜心打磨，在全体员工的共同努力下，把企业的发展与技术创新相结合，加大新技术、新业务、新市场的开发力度，不断提高企业的综合竞争实力，为数据安全建设做出更大贡献，以更优异的成绩，迎接新经济发展的机遇和挑战，促进安全产业的繁荣与发展。

虚假、仿冒 APP 乱入“江湖”

手机党们注意啦！！！

近期，国家互联网应急中心紧急发布：《2018 年我国互联网网络安全态势综述》，其中明确指出，近两年来网络诈骗行为与日俱增，其中，移动互联网恶意程序涨幅较快，威胁网民的信息安全和财产安全。

网民数量：2018 年到达 8.17 亿，其中金融服务、交通出行、支付等业务逐渐向移动互联网平台迁移。

恶意程序：移动互联网恶意程序数量 283 万余个，同比增长 11.7%。其中以流氓行为类、资费消耗类和信息窃取类为主。

2018 年通过移动应用实施网络诈骗的事件尤为突出，如大量虚假的贷款类 APP 没有真实贷款业务，被诈骗分子用来骗取用户的隐私信息和钱财。报告显示，在上述虚假的“贷款 APP”上提交姓名、身份证照片、个人资产证明、银行账户、地址等个人隐私信息的用户超过 150 万人，大量受害用户向诈骗分子支付了上万元的所谓“担保费”、“手续费”费用，经济利益受到实质损害。

此外，具有与正版软件相似图标或名字的仿冒 APP 数量呈上升趋势，通过蹭热点传播，诱惑用户下载并安装，不仅会造成用户通讯录和短信内容等个人隐私信息泄露，还有恶意扣费的隐患。

关停 APP 超 30000 个

APP 网络诈骗早有案例，国家也极其重视。自 2018 年 12 月以来，国家网信办会同有关部门，针对恶意程序、违规游戏、涉黄涉赌、不良学习类移动 APP 开展专项整治行动，关停下架违法违规 APP33638 款，拦截恶意网站链接 234 万余个，社交平台清理低俗不良信息 2474 万余条、封禁违规账号 364 万余个。

相关负责人表示，网信办将进一步加强与行业主管部门之间协同配合，共同压实网络接入服务商、应用分发平台、社交平台的企业主体责任，切断违法违规 APP 传播链条，构建全环节管理的综合治理模式，持续深入推进违法违规 APP 乱象专项治理工作，营造正能量充沛、风清气正的网络空间。

网络安全不是可有可无的工作，尽管表面看来它似乎不会为企业 / 国家创造直接效益。但是当发生了重大事故时才想起网络安全防护的重要性？对现代社会来说，网络安全已经渗透到生活的方方面面，从商业机密和客户数据的保护，到个人隐私、视频的监管，安全管理早已上升到国家战略层面，成为关系国家命脉的重要组成部分。亿赛通也时刻以保护国家、企业、个人的信息安全为己任，坚持做好中国数据安全防护专家。

调查：2/3 酒店网站存在意外泄漏顾客资料风险

据外媒报道，美国某互联网安全技术公司公布了一项针对酒店服务网站安全的调查报告。报告显示，2/3 酒店服务网站存在无意中把顾客的订房信息和个人资料，泄漏给包括广告商和数据分析业者等第三方网站的行为。

这项报告调查了 1500 多家酒店网站，调查对象包括从 2 星级至 5 星级不同档次的酒店。机构表示，几个月前，著名万豪国际集团曾爆发严重旅客资料外泄事件，此次调查并未包括万豪旗下的所有酒店。

此次调查发现旅客被泄露的资料，主要包括姓名、电子邮件地址、信用卡信息、顾客护照号码等。而网络犯罪者，对有影响力的商业专业人士、政府雇员，以及社会知名人士的个人信息资料，则越来越有兴趣。

酒店旅客个人资料外泄情况，通常会发生在酒店发送带有直接订房信息链接的确认电邮时。并且超过 30 个不同的服务商，分享过附加链接的参考码，包括社交网络、搜索引擎、广告等。

了解以上信息泄露的惨重事件后，小编只想说泄露的源头还是企业自身的数据安全保护措施不到位，如果可以完善数据安全保护建设，就不会酿成今天的悲惨结果。启用一套完善的数据安全保护方案，即使自身失误导致数据泄露，或黑客入侵，数据丢失、窃取、拿走……只要数据“打不开”，也可安全、放心。

亿赛通智能安全产品可完全防护企业数据信息，让不法分子无法查看，无法获取。产品融合数据分析、文档加密、访问控制、关联分析、数据标识等技术，帮助用户对数据进行安全治理、态势感知、智能防护；为用户的核心数据资产从终端、网络、存储、应用等全方位提供全生命周期保护，从而做到防止重要信息被有意或无意非法扩散，让用户再也不担心数据被泄密、存储不安全。

最后，亿赛通作为中国数据安全防护专家再次提醒大家，日常需注意个人隐私及企业数据的保护，不要在网上或是公共场所随意泄露自己信息内容。自身加强安全意识，筑牢安全防线。企业尽快利用起科学技术，规避泄密风险，全民行动一起抵御黑客的不法行为。

数据黑产：巧达科技非法出售 10 亿数据信息

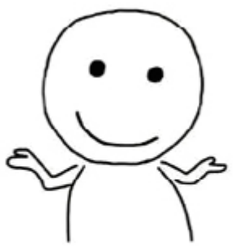
近日，巧达科技上到老板，

下到员工全体被抓。

该公司涉嫌非法盗窃用户隐私。

具体情况看亿赛通小贴士为您揭秘……

窃取个人隐私信息使用什么逼格手段？？？



这突如其来的心塞是怎么回事

犯罪背景

巧达科技号称拥有超大型简历数据库，

总数 37 亿份，

另外拥有超 10 亿份的电话通讯录。

该公司近一年就运用这些信息获利 4.11 亿人民币。

犯罪过程

巧达科技利用招聘来的爬虫工程师，

在各大招聘网站，

非法获取大量的明文简历信息，

之后通过收入分成高中低档，

每条 0.5 元 -2 元不等的价格，

批量出售给各种服务公司，

通过这样的方式，

获得一批又一批“赚钱名单”

窃密“伴侣”

除售卖给服务公司，

他们还将简历出售给你的 Boss，

该公司的 APP“爱伙伴”

可第一时间获取你的简历更新情况，

你的老板立刻就会找你“喝茶”

在信息出售之后，

你会收到各种垃圾短信、骚扰电话。

另外，还会被各种网络广告、流氓软件盯上，

始终生活在监视中。

数据安全防护小贴士犀利吐槽！！！

众所周知，

商业秘密是市场经济发展的产物，

是知识产权的重要组成部分，

也是企业重要的无形资产，

它对企业在市场中的生存和发展有着重要影响；

个人隐私也一样，

都闭嘴该我装B了！

未经加密的信息一旦被泄露，

将带来巨大的精神以及经济上的巨大损失，

所以无论企业或个人秘密被侵犯，

其后果不堪设想。

那么，

敏感信息能够被不法分子如此大批量的窃取主要来源是啥？

据调查统计分析，

80% 的信息泄露事件主要来源于企业内部，

即企业“内鬼”或者称之为“间谍”，

加之，企业对自身数据资产不够重视，

所有数据均未加密，

给“内鬼”可乘之机，

从而将获取的大量信息资产进行非法黑市交易。

近年来亿赛通为企业提供的数据安全解决方案可以看出，智能数据泄露防护的建设思路已经成为大家高度关注的焦点，围绕“什么是敏感数据？敏感数据在哪？需要控什么？需要怎么控？”等问题，构建出“数据安全智能管理平台（DSIP）”——即智能识别、智能分析、主动防护、全面监控、全面审计、风险预警……实现企业内容安全审计、介质安全管控和智能终端的安全防护，并且此方案已成功实施多家行业客户。亿赛通始终用实力、事实说话，为用户打造一个界限明确、放心可靠的数据安全环境。

大疆公司代码泄露损失百万，泄密员工获刑半年

大疆公司存在严重安全漏洞

深圳市大疆创新科技有限公司是一家无人飞行器控制系统及无人机解决方案的研发和生产商。此前，大疆的网络安全爆出严重的漏洞，该漏洞能让攻击者获取到 SSL 证书的私钥，并允许他们访问存储在大疆服务器上的客户敏感信息，这使得大疆的所有旧密钥毫无用处，从而可能导致大疆服务器上的用户信息、飞行日志等私密信息能被下载。

代码泄露：内部员工导致

经过调查，此项漏洞是大疆的一名软件工程师所为，该员工主要负责编写农业无人机的管理平台和农机喷洒系统代码。他通过一个计算机指令，将含有公司农业无人机的管理平台和农机喷洒系统的两个模块的代码上传至 GitHub 网站的“公有仓库”，造成了源代码泄露。

据悉，这些泄露出去的代码，已用于该公司农业无人机产品，具有实用性。尽管大疆公司采取了合理的保密措施，但依然给大疆造成经济损失 116.4 万元人民币。

泄露企业代码罚款 20 万

案发后，该员工删除相关代码，并积极配合调查，防止事态扩大。他在推特上表示，“无意泄露了大疆的机密”、“我很后悔自己没有法律意识，我愿意承担相应的法律责任。”

法院综合考虑犯罪情节以及自愿认罪、有悔罪表现，以侵犯商业秘密罪判处大疆前员工有期徒刑六个月，并处罚金 20 万人民币。

近期代码泄露事件频繁发生，每次都会给企业带来不可磨灭的损失。

1、 几天前，B 站的网站后台工程源码也遭恶意泄露，被一个名为“openbilibili”的用户放到了开源项目平台 Github 上。“哔哩哔哩 bilibili 网站后台工程 源码”的 repo，内容包含了项目规范和负责人信息两部分，后者还涵盖了详细的业务、具体负责人等信息。

2、 今年三月，阿里云发生因隐私权限设置错误而导致的大规模用户资料泄露事件，涉及 40 余家企业、200 余项目，只要登录阿里云旗下的云校平台，就能够浏览很多公司的“内部”代码，而这些内部代码中就包含一些用户的个人隐私信息，如身份证号、手机号、手持身份证照片等，以及企业的重要商业秘密，如销售人员报表。

3、 2018 年 10 月，西二旗某科技公司发生代码泄露。陈某是该科技公司原运维主管，通过非法手段提高自己系统操作权限，从而获取大量自己本无权限接触到的核心代码，并通过自己的账号进行下载。

以上几起案件教导我们，凡是企业代码泄露，数据均以电子文档的形式流出，并且公司内部终端都会保存大量企业商业秘密的核心部门资料。

代码泄密亿赛通有妙招

其实，代码泄露是完全可控的，只要企业从数据内部和外部两个方面进行严格管理数据，就会让不法分子无空可钻。那么针对企业机密泄露，亿赛通研发了一整套数据防护解决方案，保障数据在存储、使用、传输、外带、外发中的安全。

首先，在企业内部，以加密技术为核心，通过将技术平台与管理体系有效结合，可对任意文档自动透明加密，实现对用户核心数据资产的全方位保护。同时，通过信息安全边界的建立，降低核心数据资产如源代码、设计图纸、财务数据以及其他任意信息资产有意或无意泄密风险。此外，配合完善的信息安全咨询服务，对企业的业务进行梳理和流程建立，保障企业的核心业务正常运转，同时不影响用户工作习惯及业务效率。数据加密技术是很多公司电脑采购的标配产品。其次，在保障外发数据安全方面，针对客户的重要信息或核心资料，当员工需要将涉密文档外发给客户（代理商、合作伙伴等）人员时，应用文档外发控制系统生成外发文件发出。当外发文件打开时，用户通过身份认证，方可阅读文件。同时，外发文件可以限定接收者的阅读次数和使用时间等细粒度权限，从而有效防止客户重要信息被非法扩散。

总之，亿赛通数据防护解决方案可以实现加密数据无感知、加密数据脱离使用环境无法读取、非法获取数据后无法使用，无边界全方位保护数据安全。在信息化之路上，保障数据安全亿赛通与你一同携手共进，净化数据安全环境，让不法分子无法兴风作浪，让企业数据安全放心。

中国人民银行清算总中心牵手亿赛通 实现智能一体化安全防护

关于中国人民银行清算总中心

中国人民银行清算总中心是中国人民银行直属事业单位，是为中央银行、商业银行和全社会提供支付清算及相关服务的全国性金融服务组织，担负中国人民银行支付清算系统建设、运行、维护和管理的职责。清算中心始终不忘初心牢记使命，把“建立和完善统一、高效、安全的支付清算系统”，打造和谐支付，构建和谐金融服务环境作为矢志不渝的努力方向，扎实推进中央银行支付清算系统建设，努力提高支付清算服务水平。

需求背景

鉴于中国人民银行清算总中心计算机信息系统的应用越来越普及，生成大量的信息化文档，如银行办公资料、客户资料、业务数据等重要文档资料分散在各 PC 机上，如何保证这些重要数据的安全和实现统一安全管理，是清算中心绝对不容小视的问题。因此为维护银行信息系统的安全，清算总中心签约亿赛通共创信息安全运行新环境。

解决方案

亿赛通电子文档安全管理（CDG）系统助力中国人民银行清算总中心敏感数据安全建设：

该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产，对电子文档进行全生命周期防护，系统具有透明加密、主动加密、智能加密等多种加密方式，用户可根据部门涉密程度的不同（如核心部门和普通部门），部署力度轻重不一的梯度式文档加密防护，实现技术、管理、审计进行有机的结合，在内部构建起立体化的整体信息防泄露体系，使得成本、效率和安全三者达到最优平衡，实现电子文档的数据安全。

智能加密：可根据文档的内容进行语义识别，判断是否为清算中心所定义的加密数据并自动进行加密处理。

内容安全管控：截屏录屏控制文档、阅读水印文档、打印水印、拷贝粘贴控制。

文档权限管理：细粒度权限控制、模板批量授权、文档权限管理。

文档外发管理：用户身份认证、使用权限管控。

流程管理：文件解密审批流程、文件外发审批流程、邮件外发审批流程、离线办公审批流程、文件还原审批流程。

审计跟踪：邮件外发审计、文件解密审计、文件打印审计、流程全文检索审计、违规操作预警。

项目成果

亿赛通电子文档安全管理（CDG）系统提供对中国人民银行清算总中心内网一体化防护，保障其敏感数据安全保护，员工在使用过程中内部透明，使用无感知；外部用户非法获取内部文档无法使用；合法用户获取内部文档优先使用。完美提升等级管理建设能力，以及实现清算总中心信息安全监控、合规的要求。

慧择网联手亿赛通构筑保险业数据安全管理体系建设

客户简介

深圳市慧择保险经纪有限公司 2006 年正式成立，是经保监会早期批准获得保险网销资格的网站之一；是第三方互联网保险服务平台的创立者。经过 13 年的发展，慧择网已与 80 余家保险公司合作，提供近千款保险产品服务，产品线涵盖了健康险、人寿险、意外险、旅游险、企业险等全险种产品，服务用户超过 3000 万。

需求背景

在互联网保险运作的新趋势下，慧择网业务亦向互联网发展，产生大量的核心技术、专利、重要客户信息以及财务数据等方面的电子文档。为提高企业内部数据协同和高效运作，防止一切人为或非人为风险，实现内部文档的流转安全可控，实现文档脱离内部管理平台后能有效防止文件的扩散和外泄，因此慧择网必须加强信息安全管理。

解决方案

1、统一身份认证：支持同时同步深圳总部的 AD 域及合肥分公司 AD 域；

2、透明加密：对慧择网公司的源代码、办公软件等做透明加密保护；

3、业务系统集成：与慧择网的各种应用系统无缝集成，实现数据的上传解密、下载加密功能；

4、半透明加密：特殊岗位人员可自主选择是否加密，对公司核心部门加密文档可正常使用；

5、流程审批：对于普通员工采用流程审批解密，特殊岗位人员及高层领导分配右键特权解密功能；

6、支持手机 APP：高层领导安装手机客户端，一方面方便审批解密文档，另一方面可直接在手机上查看加密办公文档；

7、支持 MAC 端：部分高层领导使用 MAC 系统，主要是保护办公核心文件；

8、文件外发安全：对于机密文件制作外发加密文件，根据文件安全程度及外部用户可信程度设置权限，可控制是否只读、时间、次数、是否可打印等权限控制，打开认证方式可采用密码、机器码绑定、KEY 认证等方式，从而保证外发出去的文档安全控制。

项目成果

项目的成功实施大力保障了深圳市慧择保险经纪有限公司代码、财务数据、客户信息等核心数据安全；保障深圳总部跟分部合肥分公司数据交互安全，建立信息安全边界 , 有效防止企业核心信息资产外泄的同时，不影响用户工作习惯及业务效率，同时提高了员工的数据安全保护意识。

金融典型案例

1、招商银行
2、中国建设银行
3、中信银行 / 证券股份有限公司
4、中国民生银行
5、上海浦东发展银行股份有限公司
6、九江银行股份有限公司
7、宁波银行
8、泉州银行
9、中国国际金融股份有限公司
10、华夏基金管理有限公司
11、长城证券有限责任公司
12、广发证券股份有限公司
13、中国人民财产保险股份有限公司
14、泰康资产管理有限责任公司
15、新华人寿保险股份有限公司
16、山西证券股份有限公司
17、北京华控投资顾问有限公司
18、方正资本控股股份有限公司
19、润博祥北京投资担保有限公司
20、北京弘合柏基金融信息服务有限责任公司
21、北京融世纪信息技术有限公司
22、荣星（天津）商业保理有限公司
23、欧力士融资租赁（中国）有限公司
……