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

2 月刊

2019 年共 11 期

惜亡羊之阿里云端企业代码泄露

宜补牢于自身数据安全

正月，新一年的开始

数据安全防护成为数字时代的守护者

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

本刊为亿赛通企业月刊，欢迎交流，禁止转载

CONTENTS 目录

深度窥究数据安全
行业发展新走向

现如今，安全事件逐渐成为媒体的宠儿，国内外信息泄露事件此起彼伏，从未停歇，时刻牵动着众人的眼球。网络安全和信息安全已经不仅仅是一个技术问题，而是关乎普罗大众的民生问题。

近两个月来，国内知名企业电信、京东金融均发生数据泄露；俄罗斯政府、国际招聘网站无一幸免……频频爆发的泄露事件导致“数据安全”备受社会各界关注和重视。数据泄露不仅仅发生在初创企业，多数拥有数据安全防护的企业也遭遇攻击，而一个全新的、互联互通、全方位的数据安全解决方案，才是当下各企事业单位急需的安全保护网。亿赛通专注数据安全领域十六年，在今后的道路中也会继续坚守阵地，深度窥究数据安全行业发展新走向，为广大客户的数据保驾护航……

亿赛通

刊首语 PREFACE

国内

1、图片网站 500px 用户信息泄露

视觉中国 VCG

摘要：视觉中国旗下摄影网站500px发布公告称，该网站去年7月曾遭到黑客攻击，导致大约1480万用户的信息泄露。

2、非法获取公民个人信息 3890 万条 32 名被告人获刑

摘要：2012 年左右，任职于重庆某装饰公司的被告人汪某某，发现装饰行业需要大量房屋业主个人信息用于电话联系业务。汪某某将自己及公司之前收集的房屋业主信息，以及通过购买、交换等方式从他人处获取的大量公民个人信息，向其他装饰公司以及装饰公司业务员出售赚钱。

3、深圳佰仟金融工程师两毛一条贩卖隐私泄露公民信息遭到从严判处

摘要：张勇可随意调取深圳佰仟金融公司业务数据，他以每条 0.2 至 0.5 元将公民个人信息贩卖给他人，非法牟利 40.2 万元。直到被抓时，张勇的的手机和笔记本电脑里还存有公民个人信息 279.7 万条。

4、身份信息遭冒用“被法人”现象频发，致隐形公司出现存隐患

摘要：广西钦州人莫振裕去年在一次信息查询中无意中发现，自己名下竟有 130 多家公司，注册地遍布四川、黑龙江、贵州、湖北等全国各地。

5、自动获取图片侵犯隐私？京东金融致歉：已定位问题且下线修复

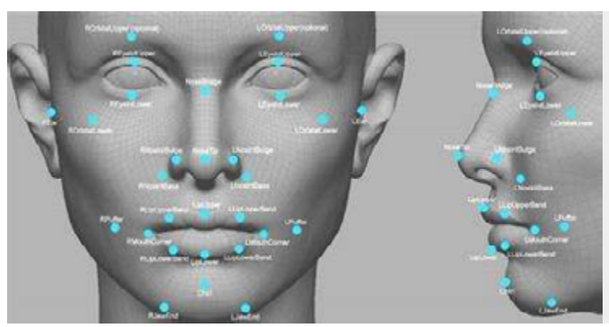
京东金融 JD Finance

摘要：2 月 16 日凌晨，一位微博网友发布了两条短视频，显示京东金融 App 会自动获取用户敏感图片并上传。京东金融解释说，上述图片缓存现象其实是其在 2018 年 12 月发布的版本中的一个便利小功能，如果用户打开京东金融 App 后进行截屏，京东金融会认为用户有可能想投诉或建议。为了方便用户和客服沟通，我们在用户界面的左上角展示图片提示，用户可进一步选择是否联系客服并发送图片。

6、央视调查：手机“黑卡”仍公开兜售，你身份证可能也沦陷了

摘要：从 2016 年开始，我国就规定使用手机必须实名登记。但长期以来，依然有一批手机卡未遵守实名制的规定，未实名或假实名，被称作手机黑卡。这样的手机卡也成了犯罪分子最热衷的作案工具，因为即使警方追踪到了手机号码，也难以追踪到犯罪者本人。这些虚拟运营商的卡，用户只需要在网上上传身份证就能办理，用别人的身份证也能通过。

7、超过 256 万国人数据库“裸奔”半年多，包含人脸识别信息



摘要：日前，国内一家面部识别公司的数据库暴露在网上，且无密码保护，其中包含超过 256 万人的重要信息，包括人脸数据。

8、中介违规网签 房子难以售卖究竟谁的错

摘要：王女士去年 3 月开始售卖自己的房子，5 月底，收完购房者的 40 万定金后办理过户时，却遭到工作人员的拒绝，工作人员表示房子已经办理过网签，现在不能过户了。经过查明，提交网签手续的是当地一房地产中介公司，但王女士称，自己并未授权该中介公司进行网签。

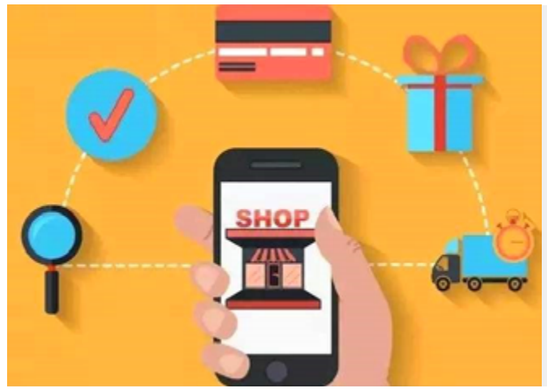
9、长春纪委：一民警提供公民个人信息，致犯罪组织实施强迫卖淫

摘要：2016 年 5 月至案发，民警杨凯鑫利用工作便利，长期违规使用西三条派出所所长赵嵬的公安信息系统数字身份证书，将从公安信息系统获取的公民个人信息提供给金威臣黑社会性质犯罪组织，致使其有组织地实施强迫卖淫、非法拘禁等违法犯罪活动，并为金威臣等人充当“保护伞”。

10、中国的数据保护正日趋成熟？

摘要：Smaato 亚太区董事总经理 Alex Khan 表示：“当今这个时代，数据隐私无疑是最重要的，但在中国却并非如此，因为目前还没有任何组织或政府机构来监管数据安全。但 [这] 并非没有好处。监管的缺失让收集的数据被更好地利用，支持了更深入的洞察，从而形成了更健康的生态系统。”

11、个人信息安全规范草案：用户应有权拒绝个性化推送



摘要：日前，全国信息安全标准化技术委员会开展国家标准《信息安全技术个人信息安全规范（草案）》（下称《草案》）征求意见工作。《草案》要求，不得强迫收集个人信息，用户应有权拒绝个性化推送。

12、《流浪地球》等电影资源泄露 国家版权局出手打击

摘要：大年初二开始，《流浪地球》《疯狂的外星人》《飞驰人生》等春节档大片就齐刷刷在网上出现高清盗版资源，被业内称为“中国电影史上最大泄露事故”。2 月 10 日，国家版权局发布声明，表示将严厉打击网络侵权盗版，保护优秀国产电影，对严重的侵权盗版分子，将移交公安部门采取刑事手段予以严厉打击。

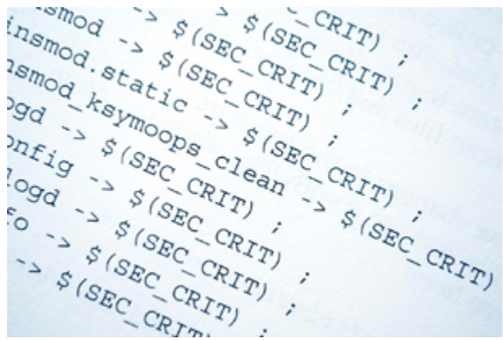
13、下载 App 时谨慎点击“同意” 提防过度授权导致信息泄露

摘要：通话记录、公积金数据、微信余额、支付宝账单……这些看似非常隐私的数据，很有可能因为用户在注册一些 App 时同意注册协议以及授权，轻而易举地到了一些大数据公司手里。而经过大数据公司利用科技手段进行“包装”之后为个人生成的一张张画像，又以几元到几十元的价格，被卖给了其它一些需要个人信息的平台，或许这就是为什么一些陌生人对自己这么熟悉的原因之一。

14、“号码百事通”数据库遭外泄，2 亿余条个人信息被卖

摘要：近期浙江有一起侵犯公民信息案，从各方面刷新了人们对这个黑色产业的认识——该案非法获利金额累计达 2000 余万元，涉及公民个人信息 2 亿余条。这些信息流出的源头陈某，曾经是中国电信分公司、号码百事通（以下简称“号百”）服务有限公司部门负责人。

15、盗取公司源代码，获刑 5 年罚 400 万



摘要：“内鬼”盗取游戏源代码后设立公司，利用该代码上线、运营游戏营利，直至案发，游戏玩家总数达 14 万余人，游戏充值金额达 8000 万余元。1 月 22 日，由成都高新区检察院依法提起公诉的这起侵犯网络科技公司游戏源代码著作权案宣判，被告人邱某被依法判处有期徒刑 5 年，罚金 400 万。

16、非法广告搜索排名 网络黑产链一年牟利上百万

摘要：2018 年 2 月初的一天，如东县公安局接到辖区一家公司报警，称公司网页遭到黑客攻击。据该公司网络维护人员反映，这一段时间感觉公司网站的响应速度有所降低，但网页内容没有任何异常。他们查询网站后台才发现，在眼花缭乱的数据代码中，居然被人植入了“一句话”。而根据这句话的内容进行检索，找到的是一个招嫖网站。

17、收房后业主频遭电话推销：绍兴装修业等 16 人涉侵犯个人信息

摘要：2018 年 11 月，羽林派出所接到多名市民报案，称所在小区刚交付就频繁接到电话推销，怀疑个人信息泄漏。根据小区居民提供的信息，警方锁定当地一家装修公司负责人袁某，在其办公室搜出印有某新建小区 500 多名业主个人信息的打印纸，包括姓名、房号、面积、电话、身份证号等。

18、花总维权两月仍不知信息泄露源头：非常难受只能死磕

摘要：2018 年 11 月，微博网友“花总丢了金箍棒”（以下简称“花总”）曝光酒店卫生乱象，引爆舆论。仅仅几个小时之后，花总的个人信息被一家酒店的员工曝光在网上。

19、房地产领域泄漏用户信息 诸暨检方提起行政公益诉讼

摘要：2017 年 12 月，小朱刚刚买了一套婚房，没多久，便开始接到各种各样的推销电话，一天少则一两个，多则五六个，从售楼商铺到装修设计，从家居建材到小额贷款，电话那头不但能准确地说出小朱的姓名，甚至连其购买的楼盘房号也一清二楚。

20、长沙辅警龚某联手 25 名房产中介违规售卖户口，26 人均获刑

摘要：长沙某地产公司的销售顾问罗某是个“能人”。只要给他相应资料，他就能在一定时间内，帮人弄来“长沙户口”。罗某为何有这么大的能耐？原来，他与辅警龚某“合作”，以每本三四千元的价格，让龚某帮忙给人落户。之后，他再转手卖给其他房屋中介。

国外

1、黑客入侵 POS 公司系统，在客户网络植入恶意软件

摘要：总部位于明尼苏达州的 POS 产品供应商 North Country Business Products（NCBP）上周公开了一个安全事件：黑客入侵了其 IT 系统，后来在其部分客户的网络上植入了 POS 恶意软件。

2、印度国有液化石油气公司 670 万用户信息遭泄露，包括 Aadhaar 号码

摘要：近日，法国安全研究员在一名不愿透露姓名的印度安全研究员的帮助下发现了印度国有液化石油气公司 Indane 官方网站的一个安全漏洞。该漏洞被证实会导致数百万用户的个人信息泄露，包括他们的 Aadhaar 号码。

3、前美国情报人员被指控从事间谍活动以及向伊朗黑客提供帮助

摘要：美国司法部于上周三（2 月 13 日）正式宣布对一名前美国空军情报官员提出间谍指控，这名官员被指在 2013 年叛逃到伊朗后向伊朗政府提供了与美国国防有关的文件和资料，且有理由相信这些文件和资料可被用来损害美国的利益并使伊朗获利。

4、新 Astaroth 木马病毒可利用杀毒软件窃取数据

摘要：Astaroth 以其最新的形式出现在巴西和欧洲的垃圾邮件宣传活动中，截至 2018 年底，已有数千受害者设备被感染。恶意软件通过 .7zip 文件附件和恶意链接传播。木马伪装成 JPEG、. gif 或无扩展文件，以避免在机器上执行时被发现。

5、VFEmail 遭遇毁灭性攻击，大部分数据遭到破坏

摘要：总部位于美国密尔沃基的电子邮件提供商 VFEmail 遭遇了一场“灾难性”攻击，导致其美国境内服务器上主要和备份系统上的所有数据被破坏。

6、16 家国外热门网站数据疑似被盗，近 6.2 亿条账户信息被挂暗网出售

摘要：据英国科技新闻网站 The Register 报道，暗网交易市场 Dream Market 于本周一（2 月 11 日）挂出了这样一条广告——卖家声称自己手里掌握着约 6.17 亿条从 16 家国外热门网站盗来的账户记录，而买家只需要支付价值不到 2 万美元的比特币就可以得到所有这些数据。

7、RDM 制冷系统曝严重安全漏洞，全球众多医院、超市受影响

摘要：Resource Data Management(一家位于苏格兰的远程监控解决方案公司)制造的制冷系统存在重大安全漏洞，英国、澳大利亚、以色列、德国、荷兰、马来西亚、冰岛以及世界其他国家共发现了分布于数百个不同地点的 7419 台易受攻击设备（医用冷藏柜、超市冷藏柜、冷冻库等）。

8、俄罗斯遭遇新一波垃圾电子邮件轰炸，旨在传播 Shade 勒索软件

摘要：在 2019 年 1 月的监测中，ESET 公司的安全专家发现了大量采用俄文编写的垃圾电子邮件，它们旨在传播一种被称为“Shade”（或“Troldesh”，由 ESET 检测为 Win32/Filecoder.Shade）的勒索软件。

9、疑似俄罗斯政府“后门账户”暴露，可用于访问数千家企业的服务器

摘要： 据外媒 ZDNet 报道，一名荷兰网络安全研究人员于近日在偶然间发现了一个疑似由俄罗斯政府使用的后门账户，这个后门账户是他在审查数千个因为没有设置密码而暴露在互联网上的 MongoDB 数据库时发现的，任何注意到这个账户的黑客都可以使用它从在俄罗斯经营的数千家企业获取敏感信息。

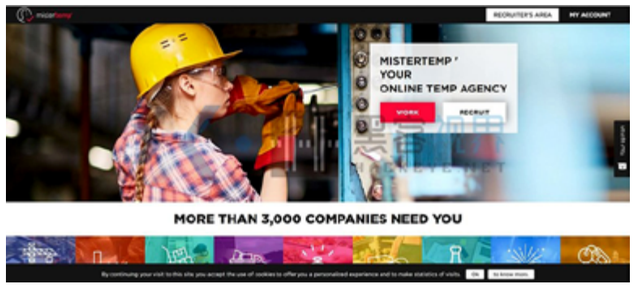
10、新加坡 1.4 万艾滋病患者个人健康信息遭泄露

摘要：新加坡卫生部（Ministry of Health，MOH）于发布消息称，数千名被确诊为 HIV 阳性患者的新加坡人和外国人的医疗记录和联系方式现已经被公开发布在了网上，此次个人健康信息遭到泄露的艾滋病病毒携带者大约有 14200 名。并表示，这些信息全都掌握在美国公民米基·K·法雷拉·布罗切兹（音译，Mikhy K Farrera Brochez）的手中。

11、PHP PEAR 网站遭黑客入侵，官方软件安装包被篡改

摘要：PEAR 的维护人员发现有人用核心 PEAR 文件系统中的修改版本替换了原来的 PHP PEAR 包管理器 (go-pear.phar)，尽管 PEAR 开发人员仍在分析恶意包，但根据他们 2019 年 1 月 19 日发布的一份安全声明，因被黑客入侵，网站被恶意代码感染的安装文件至少已存在半年。

12、招聘网站数百万条敏感数据泄露，简历、身份证扫描件统统曝光



摘要：据外媒报道，国际网络安全咨询公司 HackenProof 的安全专家在 2018 年 12 月 21 日发现了另一个没有得到很好保护的 Elasticsearch 集群，其中包含数百万非常敏感的数据记录。从索引的名称来看，它的所有者毫无疑问就是 MisterTemp。这是一家法国临时工招聘网站，声称任何人都可以通过该网站快速申请一份临时工作，并能够提供来自法国全国范围内不同行业的临时工作机会。

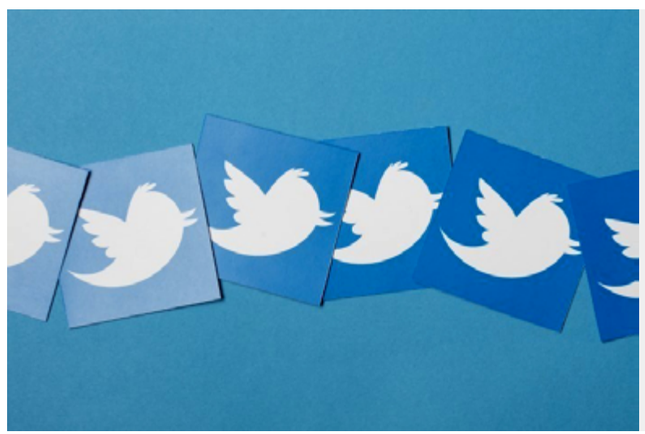
13、美国多个赌博网站泄露一亿余条投注信息

摘要： 安全研究员发现了暴露且难以实施保护的 ElasticSearch 数据库，但当时研究者未能确定该服务器的管理者，所以联系了托管服务提供商以便它可以得到保护。数据库似乎包含了许多在线赌场的投注信息，这些赌场提供传统游戏，以及允许玩家通过玩游戏赚钱的街机类游戏。公开的数据包括投注者的个人信息、推荐他们访问该网站的关联公司、他们的余额、存款、取款和投注。

14、MySQL 设计 Bug 允许恶意服务器从客户端窃取文件

摘要：客户端主机和 MySQL 服务器之间的文件传输交互中的设计缺陷允许运行恶意 MySQL 服务器的攻击者访问连接的客户端具有读取访问权限的任何数据。不法分子可以利用此问题从配置不当的 web 服务器 (允许连接到不受信任的服务器) 或数据库管理应用程序检索敏感信息。

15、Twitter Android 版被曝存在 Bug，暴露用户私人推文



摘要：Twitter 公布了一项安全问题，这个问题导致 Android 设备上用户四年内发送的私人可见的 Twitter 内容变得完全公开。Twitter 表示，如果 Android 操作系统上的 Twitter 用户在过去四年中对其帐户设置进行了特定更改（例如更改与其帐户关联的电子邮件地址），则“保护您的推文”设置将被禁用。这意味着原本展示给私人用户的推文内容实际上对公众开放。

16、美俄克拉荷马州证监会数百万份文件泄露，最早可追溯到 1986 年

摘要：网络安全公司 UpGuard 的数据泄露研究小组披露了一起严重的数据泄露事件，一台被用于存储美国俄克拉荷马州证监会（Oklahoma Department of Securities，ODS）数据的服务器因为没有受到很好地保护，导致共计 3TB 大小的数百万份文件可公开访问。

17、韩国防采办计划管理局遭黑客入侵，下一代战斗机采购计划疑似被盗

摘要： 近日，韩国当地媒体《东亚日报（Dong-A Ilbo）》报道称，一群未知黑客成功侵入了该国国防采办计划管理局（DAPA）的 10 台电脑，而这一消息很快得到了韩国国防部的证实。

18、把资料放在网盘的风险有多大？MEGA 网盘 87GB 数据遭泄露

摘要：澳大利亚知名安全研究员通过自己的个人网站发文称，有多位粉丝在上周与他进行了联系，告知他“深受欢迎的云存储服务 MEGA 无意间暴露了大量的文件”。经 Troy Hunt 证实，遭泄露的文件超过 1.2 万个，包含 87GB 的数据。

19、美国德尔里奥市遭遇勒索软件攻击，政府工作人员重回纸笔办公

摘要：据外媒报道，位于美国德克萨斯州的德尔里奥市遭遇了一起黑客攻击，该市市政厅的服务器因感染勒索软件被迫离线，进而导致电子政务平台停止运行、市政厅工作人员不得不重新使用纸和笔来进行办公。

20、美国宇航局 NASA 内部软件暴露了员工和项目信息

摘要：安全研究员发文称，美国国家航空航天局（National Aeronautics and Space Administration，NASA）内部使用的一款 Web 应用程序因为存在人为配置错误无意间暴露了员工用户名、姓名、电子邮箱地址和项目名称等详细信息。

亿赛通副总经理：张磊

随着 2017 年《中华人民共和国网络安全法》的正式实施，再到 2018 年 5 月欧盟《通用数据保护条例》(简称 GDPR) 的出台，数据信息安全在一定程度上得到了法律法规的制约。

然而回看 2018 年，频频发生的重大企业信息泄露事件，一度成为信息安全领域的热门话题，备受社会各界的关注和重视。其中数据泄露已飙升为常见的网络安全事件之一，给企业和个人带来了严重危害。随着大数据时代的到来，数据资产释放出无限商业价值，数据安全受到严重威胁。

数据安全防护成为数字时代的守护者

比特专访节选

数据因价值而变的危险

当前，数据价值已经成为与物质资产和人力资本同样重要的基础生产要素，数据安全成为企业健康发展的核心要素，催生了数据安全防护市场的增长。

在此契机下，亿赛通逐渐将业务重点从文档加密转移到数据安全防护。强化产品技术，持续研发新产品。2016 年，亿赛通完成了各终端模块的打通，2017 年发布全新的数据安全智能平台 (DSIP)，将数据安全技术与产品整合，实现对安全事件快速响应和主动攻击。

亿赛通副总经理张磊在接受采访时表示：数据安全防护面临的挑战内因主要体现在人的安全意识。人为的恶性攻击相对自然灾害而言显得更为复杂多变。亿赛通组建数百人的服务团队，其中咨询团队负责现状调研，针对不同情况对企业开展思想安全意识培训，从根源上解决企业诟病。外因则是体现在企业的数据安全防护措施，以产品作为辅助工具加强企业安全防御，通过服务 + 产品形成一体化服务解决当下问题。

在业内，主流安全厂商大致可分为三类。第一类，传统安全厂商。业务偏向于攻防，注重网络和边界安全；第二类，专注特定产品研发，深耕某一行业；第三类，国外安全厂商。由于国外法律法规相对健全，很少有厂商做加密产品。在张磊看来，亿赛通更加注重内在安全，与前两类厂商形成互补。与国外厂商相比，亿赛通拥有安全自主可控的产品，在国产化方面更具竞争力。

近年来，亿赛通为国内外众多企业提供数据安全解决方案。与京东方签署了千万级的项目、中国 46 个海关单位建立合作、格力集团全业务线签署战略合作协议等。为金融、能源电力、运营商、党政军、设计制造、研发通讯等八大行业，数万家企业及 400 余万终端用户铸就了坚不可摧的安全盾牌。亿赛通以数据安全、网络安全及安全服务三大业务并驾齐驱，在安全市场中占有重要地位。

安全人才培养是关键

随着亿赛通业务的不断壮大，北京研发中心不足以支撑公司的发展速度。2018 年初，武汉第二研发中心成立，正式开启北京、武汉双核研发驱动模式，为企业发展和人才培养注入源源不断的活力。武汉研发中心的成立不仅缩短了项目交付时间，还推进了华东、华南、西南地区客户业务运转。此外，在 2017 年底成立项目管理办，负责管理项目和培训渠道代理商。亿赛通研究院又与多所高校结成“产学研”联盟，把实践教学基地建设成为校企之间合作的桥梁和纽带，储备高素质、高效率、创新型的专业人才。

2018 年，亿赛通以夯实基础为渠道建设出发点，以等级梯队制度为技术迭代落脚点。2019 年，亿赛通将深度探索如何创新，加大研发的投入和新方向的探索。张磊谈到：开源是一个公司发展壮大的重要因素，也会带来大量机会，但如何将商业机会转化成业务增长点将是我们 2019 年的重担。

大数据正在重塑世界新格局，而数据泄露事件却在持续增长。如何才能在数字时代更好地生活和工作成为个人和企业日益思考的问题！亿赛通的目标是成为数据安全厂商，它正在安全防护市场上扮演着保护数据所有者信息资产安全的卫士角色，为企业数据安全保驾护航。希望亿赛通的改变能够影响整个行业。

数字转型·智创未来，中国 IT 市场年会亿赛通连续多年荣获“年度成功企业”奖

2019 年 2 月 28 日，由中国电子信息产业发展研究院主办，赛迪顾问股份有限公司承办的 2019 中国 IT 市场年会于北京香格里拉饭店圆满落幕，本次大会以“数字转型·智创未来”为主题。会议邀请了 IT 界千余著名企业精英人士参会。亿赛通作为中国数据安全防护专家一直以专业的态度、过硬的产品以及丰富的解决方案傲立于数据安全市场，连续多年获得赛迪权威机构认可，被赛迪研究院高度关注。2019 年中国 IT 市场年会亿赛通再次荣幸受邀参会，并被授予“2018-2019 中国数据防泄露 DLP 市场年度成功企业”权威奖项。

亿赛通连续四年荣获成功企业奖

年会现场，亿赛通与众多 IT 界著名企业共同探讨了 IT 行业新动态、关注数据应用领域的发掘、市场创新方向的开拓，以及 IT 产业创新环境的重塑。身为数据安全行业的先锋企业，为了做好、做精每一个项目，亿赛通特别组建专业研发团队，并注重积累、消化、升级每一次实施经验，对安全问题、服务精确了解，使得公司能够较为全面、深入地了解客户需求，开发出符合行业需求特点的产品。产品和服务的不断完善升级，获得了客户的满意，从而为亿赛通在数据安全市场奠定了坚实的基础。市场的广泛赞可让亿赛通在本次中国 IT 年会上再次拿下“2018-2019 中国数据防泄露 DLP 市场年度成功企业”奖项。

如今，随着新一轮信息技术革命的爆发，数字技术与行业应用价值不断释放，以人工智能、大数据为代表的新技术不断应用于设计制造、金融、能源等行业，其作用不断凸显。政府高度重视数字转型发展，大数据产业的发展现状和趋势对安全要求越来越高，需要安全厂商具有更开阔的视野、更积极进取的心态和敢于担当的勇气，紧密配合发展的实际，为数据转型发展提供有利的支撑。

作为国内一流的数据安全产品提供商，亿赛通将聚焦突破，拥抱变化，加强安全产品研发，坚持专注数据安全行业，为国内外企业不断提供行业解决方案，保障企业实现数据资产安全。保护数据安全，亿赛通竭诚与您携手共进，继续做好中国数据安全防护专家。

2019 新春年会 -- 感谢有你，亿赛通开启新年新篇章

感谢 365 天风风雨雨的陪伴；

感谢一年辛苦如一日的付出；

感谢每一位亿赛通人的一路同行；

亿赛通的今天，

离不开大家的共同努力。

1 月 25 日，亿赛通新春年会盛大举办，

睁大你的眼睛，

带你观赏，

不一样的年会风景！

年末是收获的季节，

是对员工全年辛苦工作的肯定，

本届年会中颁发了：

优秀新人奖　优秀员工奖

公司的成功离不开你们勤劳的奉献

管理之星　研发之星　销售之星

管理层、技术和销售的中流砥柱

优秀团队奖　杰出团队奖

项目的成功依靠你们的辛苦贡献

感谢有你，一路同行（五年奉献奖）

五年与亿赛通风雨同舟，见证公司的成长

年会现场，

同时充分证明了，

我们是，

上可工作拿奖， 下可嗨翻全场。

年会必不可少的环节就是红包雨，

各种红包大奖，

统统带回家！

所有员工疯狂呐喊，

BOSS 们，快用钱砸我们吧！！！

伴随着年会“传统”

亿赛通 2019 新春年会进入尾声，

感谢有你，一路同行，

亿赛通大家庭的心始终与你们同在！

校企深度融合，亿赛通着力推进“双师型”人才培养

为贯彻落实党的十九大及市委第十二次党代会精神，进一步深化北京职业教育改革，坚持立足需求、提升质量、优化布局、城教融合、协同发展的思路，构建完善现代职业教育和培训体系，强化高等院校与企事业单位的“产学研”合作，推进校企深度融合，培养大批高素质技术人才。中关村战略新兴产业职业教育集团特于2019年1月15日举行了”双师型“教师企业实践基地授牌仪式，为提升北京城市治理水平和服务品质、促进产业转型升级和经济社会发展、构建和谐宜居之都提供有力支撑。

随着社会发展的步伐日益加快，人才储备已经成为企业的核心竞争力。本次培训基地评选仅有五家企业入围，由于亿赛通作为海淀区高新技术企业，此次榜上有名，初批被授予此项荣誉。我司一直与高校保持紧密合作，曾与多个高校共创网络安全实践教学基地，将数据安全的人才培养付诸社会技能实践当中，企业和大学共同培养人才，为我国数据安全的人才储备贡献自己的力量。

亿赛通将以实践基地为契机，深入研究，使人才培养和社会实践紧密结合，储备高素质、高效率、创新型的专业人才。开展挖掘更广阔的合作空间，把实践教学基地建设成为校企之间合作的桥梁和纽带。企业充分利用这次机会，发挥自身优势，积极开展形式多样的人才合作与交流。同时，亿赛通也一定会为高校提供力所能及的服务，为学生的实习锻炼提供便利，为高级人才提供实践平台，真正促进企校合作，实现双赢！

亿赛通作为中国数据安全防护专家，依托于企业16年发展历程，拥有丰富的产品线、专业的技术人才。未来通过培训、指导、作业三个阶段，在校企合作中加强基地的实质性工作建设，帮助学生积累经验，夯实专业功底，全面提升个人综合素质和职业能力，培养坚忍不拔、严谨细致的工匠精神，为自己的美好未来而努力；为数据安全领域培养锻炼、积累储备所需人才；为国家和社会的发展贡献自己的青春力量。

亿赛通喜获海淀园工会多项荣誉

2018 年，亿赛通在上级工会的大力支持下，企业工会紧紧围绕公司发展目标，强化自身建设，结合自身特点，充分调动职工的积极性，开拓进取，与时俱进全方面落实依靠方针，组织职工积极开展活动，推进企业民主管理，进一步增强企业凝聚力。

在中关村海淀园工会组织的 2019 年工作会中，亿赛通被海淀园工会授予“先进企业”、“先进基层工会”及“北京市职工书屋示范点”等多项荣誉，对企业工会在 2018 年的相关工作给予表彰！对亿赛通而言，员工是企业重要的组成部分，是企业运行、发展的原动力！只有让员工保持良好的工作状态，为员工提供适宜的工作环境，才能让企业持续、健康发展。

亿赛通工会在 2018 年深入贯彻国家政策，发挥企业人才优势，并结合自身情况，坚持落实工会工作部署与方针政策，努力完善公司工会各项规章制度，为工会每一位员工谋取福利。

在海淀园工会的正确引导下，亿赛通努力推进完善公司文化建设，满足职工基本文化需求，组织开展工会活动，丰富职工日常工作与生活，切实加强职工思想道德修养、提高文化知识水平、科学文化素养与职业道德修养。2018 年，企业工会在各大重要节日为员工发放节日礼品，职工书屋统计员工需求新增图书，为职工送去工会组织的温暖。不定期举行诸如户外活动、团建等一些提升员工身体素质的活动，增加企业凝聚力。

2019 年，亿赛通工会将继续全面配合海淀园工会工作部署，以维护公司职工合法权益为基本职责，发动和组织职工完成公司工作任务，积极开展文体活动，提高职工思想政治素质和文化技术素质；继续像更多的企业工会学习，在遵循企业文化的同时让每一位工作者都能够在亿赛通的舞台尽情施展才华，从而促使企业不断注入新鲜血液，将亿赛通工会推向一个新高度。

亿赛通再次荣登“中关村高成长企业 TOP100”榜单！

近日，由北京中关村高新技术企业协会主办的“2018 中关村高成长企业 TOP100”评选活动圆满落幕，北京亿赛通科技发展有限责任公司凭借在解决方案、态势感知、安全服务多层面的优势，获得评委会专家一致认可，成功入选后再次获评。

据悉，“中关村高成长企业 TOP100”推介活动自 2009 年创办以来，已成功举办了八届，在各级政府及主管单位的专业指导和大力支持下，成为北京中关村地区权威性和公信力双全的大型公益性评选活动之一。

在总结以往经验的基础上，本届活动秉持“自主、自愿和公平、公正、公开、公益”的“四公”原则，甄选具有核心技术、创新能力强、发展速度快、拥有良好发展前景的企业，并对企业的社会责任感和持续成长能力有明确要求。亿赛通作为在中关村成长壮大起来的企业代表之一，成功获评。

2018 年，亿赛通继续以“服务客户、持续创新、勇担责任、专业至上”的核心价值观，坚持创新研发核心技术，深深扎根于数据安全一线。其专业安全服务团队不负使命，出色完成了 DSIP、数据库审计、勒索病毒防护卫士等多项新产品研发。

本次 ,亿赛通入选“2018 中关村 TOP100 高成长企业”，是主办方和各领导单位对公司在数据安全领域成绩的肯定。未来，我司将继续深耕安全领域，进一步发挥自身在数据安全解决方案和服务上的优势，不断向着“保护数据所有者的信息资产安全”的愿景前进。

海淀区国际商会表彰亿赛通“2018 年度优秀合作伙伴”

精诚合作，立创佳绩

近期，北京市海淀区国际商会为感谢长期以来一直与其相互支持、信任的合作伙伴，特设置并颁发“2018 年度优秀合作伙伴”奖项。获此奖项是亿赛通与商会长期友好合作的强力见证，是商会对我司能力的极大认可。

在数据大规模泄露、资金被盗、业务中断等事件频频发生的大背景下，亿赛通与多协会、企业合作，帮助合作伙伴守护其内部核心数据资产，斩断数据泄露源头，加强内部的数据安全防护。无论从核心技术方面的创新，还是从信息安全解决方案的优化，亿赛通一直坚持在数据安全领域做出突出贡献，对促进我国安全和服务创新具有重大意义。

此次，亿赛通获得这一殊荣与海淀区国际商会的信任和支持是分不开的。我司秉承着“中国数据安全防护专家”的口号，守护国家、企业及个人的信息安全，以“提供有竞争力的数据资产安全解决方案和服务，持续为客户创造价值”为使命，打造完善安全的解决方案，两家合作理念相通，在合作的过程中彼此信任，相互支持，优势互补，真正形成了强强联合的优势。

亿赛通作为海淀区国际商会的合作单位 ,一直坚持着“信用为本”的原则，用实力践行一个企业的责任。自成立以来，亿赛通深受企事业用户信赖，无论在企业信誉还是发展前景方面，一直自觉遵守信用基本准则、自愿接受公众对亿赛通公司的监督，努力产生示范效应，带动相关公司信用环境的改善和各项建设事业的发展，树立良好信用品牌。同时凭借良好的经营模式，以及企业的优良业绩，在行业中，拥有很好的品牌认可度和忠诚度。在不断的钻研中，亿赛通在数据安全市场领域更加专业与成熟，并且在行业的持续发展中，企业较为稳定。因此，商会在众多合作企业里，亿赛通凭借自身的优势、品牌以及实力，一举夺得“2018 年度优秀合作伙伴”荣誉称号。

未来，亿赛通将继续发挥自身优势，为各企事业单位提供满足不同客户需求的行业解决方案，为各行业客户信息安全提供强有力的保障。

脚踏实地，守护安全！亿赛通专业服务获长城汽车高度赞扬

近日，亿赛通为长城汽车股份有限公司提供的优质服务与技术支持获得客户高度赞扬，特发来表彰！

双方合作过程中，亿赛通积极主动的工作态度和高效的应急服务受到长城汽车的高度认可。据悉，长城汽车在数据防泄漏项目启动过程中进行了大量调研，面向全国招标，针对多家厂商的安全产品进行筛选测试。亿赛通从长城汽车的实际需求出发，量身定做出适合企业的数据防泄密解决方案。

项目自启动以来，获得亿赛通高度重视。由于公司产品功能强大且易于使用，经过项目前期测试后，长城汽车所有终端均上线数据防泄漏产品，以保障公司内部文件加密管控，并在所有涉密终端上无障碍流转，从而促进了长城汽车在项目过程中建立跨部门协作，提高内部共享效率的同时，确保文件安全。

亿赛通公司在此项目中依托数据安全行业多年积累的技术经验，充分发挥技术资源优势，组织了专门的技术团队，在项目实施过程中保证长城汽车业务安全运营。过程中遇到问题，亿赛通均以高效、专业的售后服务体系积极响应，对问题进行及时处理。无论是线上售后技术，还是一线工程师均全力配合项目进行，克服自身困难、坚守一线、现场或远程为长城汽车排忧解难，加班加点完成任务，保障项目进度，并针对其日常运维及系统架构优化提出改进意见。亿赛通工程师精湛的技术以及快速响应服务有力保证了长城汽车数据防泄密系统的使用，得到其公司领导的肯定！

除长城汽车外，亿赛通多年以优质的服务全力配合各大企业数据安全防护工作，在业内更是屡获赞誉。这些赞扬，既是我们的荣幸，也是继续前进的动力！未来，亿赛通会再接再厉，脚踏实地，用专业、高效的产品和服务回报广大客户，在后方继续支撑企业数据防护工作，为数据安全建设做出更多积极贡献！

超 2 亿简历正在“裸奔”，你中招了吗？

又是一年求职季，

一份好的“简历”是求职的先决条件，

求职者都会在简历中费尽心思，

只为获得企业青睐！

简历中包含多项个人私密信息，

姓名、住址、联系方式、工作经历等等……

甚至有的求职者会将身份证号码放在简历中，

大量的个人信息使不法分子蠢蠢欲动 ~

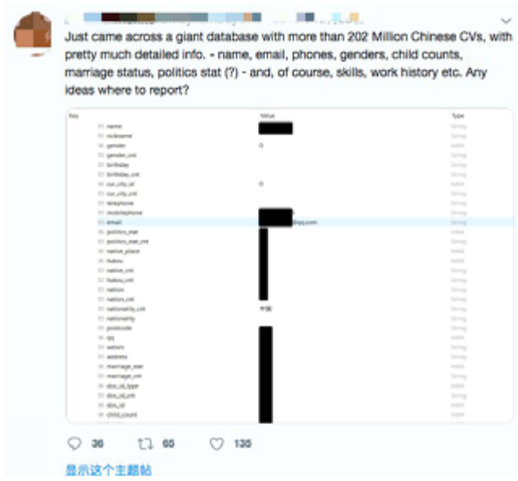
近日，国外某社交平台爆出，

“2.02 亿中国人简历信息泄露”

What ！

如此庞大的数字，

瞬间让求职中的小伙伴坐不住了。



据悉，爆料者为国外安全研究人员，

截图中可清晰看到，

姓名、电话、生日、政治面貌和工作经历等信息。

有网友直接在推文下询问：

“数据的所有者是谁？”

爆料者回应：

“不知道，

数据存储于亚马逊云服务平台上 ,全部都是简历信息。”

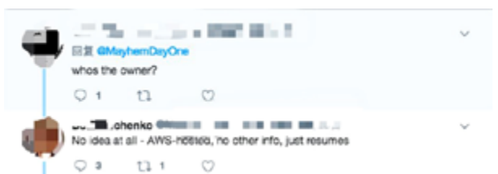
除此之外，还有网友评论，

“只想安稳找个工作怎么这么难？”

“简历泄露该谁负责？”

更有甚者回复：

“能否将数据分享？”



what are you 弄啥咧

其实关于简历数据泄露的消息并不少见，

18 年国内某知名招聘网站就爆出曾泄露 195 万条简历信息。

对此，

中国数据安全防护专家亿赛通想说：

求职者选择招聘平台时，需谨慎上传个人信息；

账户密码应定期修改并设置复杂密码；

不同平台设置不同密码；

但这些也只是减轻信息泄露而已，

要想从根源减少事件的发生概率，

还需要企业有关部门加强管理，

防范此类事件再次发生！

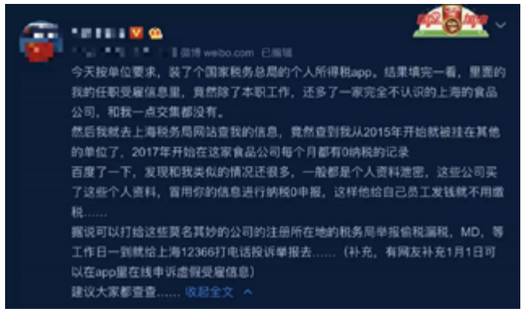
亿赛通愿与各大企业一起守护您的信息安全 ~

网友莫名其妙“被入职”，背后身份信息到底何去何从？

12 月底，个税正式开始网上申报。不过，申报刚刚开始个税就“摊上大事儿”了，有网友表示，在填报个人信息时，发现“被入职”一家从未见过的陌生企业。

某网友在其个人微博反映：“装了税务总局的个人所得税 App。结果填完一看，里面的任职受雇信息里，除了本职工作，还多了一家完全不认识的食品公司。”经过核实，是因为该网友曾给别人写过东西，他们通过第三方的人力资源公司帮开稿费。

对此，相关专家表示，这位网友的个人身份信息很可能被泄露，才导致被个别企业进行虚报个税，以达到偷逃企业所得税的目的。举例来说，某企业多为一名这样的“影子员工”虚报一份不存在的“工资”，就可以在缴纳企业所得税时多抵扣一份。



其实，从很早开始，类似现象就层出不穷。

2018 年 9 月，常州大学某学生就曾发现还未找到工作的他，竟然已经率先交了税。学校也在后续调查中发现，有 2600 多名同学信息被泄露导致提前已申报月薪交税，占据该学校总人数的三分之一。

2017 年，南京理工大学泰州科技学院也出现过类似爆料，学生反映江苏某保险代理公司盗用了他们的个人信息，疑似用来偷税漏税。在微博、微信等社交平台内，还有江苏无锡、云南昆明等地的学生均透露有过类似遭遇。

……

针对某企业获取个人资料制造”影子员工“等问题，小编在此向各位 boss 普及一点小知识：通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。因此，不管企业是否存在信息买卖行为，在本人不知情的背景下利用其信息虚报工资，已经涉嫌非法提供和获取公民个人信息，涉嫌犯有侵犯公民个人信息罪。

另外，对于盗用个人信息企图偷税漏税的情况，即使相关部门都快速作出反应，但措施大都局限在“事后”解决上。所以，还是需要从源头消除类似事件发生，要将安全意识和技术手段结合起来共同保护个人信息。亿赛通曾与众多重要行业携手打造客户信息安全，既保证企业业务较高的可用性、可靠性、保密性，又对内部核心数据有较强的防御、管控能力，如电子文档安全管理系统，实现了企业内部电子文件的加密存储。无论是由人工生产还是由应用系统生成的，只要写在磁盘上就是加密形式，倘若未经合法许可将加密文件数据体带走，加密文件内容将不能够被正常打开，从而确保文件内容不会因为文件数据扩散而泄密。

亿赛通数据安全管理体系可以有效支撑企业信息管理业务，提升内部信息安全工作的发现、管理能力与处理效率，为数据安全贡献重要技术力量。保护隐私信息安全，亿赛通从不懈怠，一直坚持做好中国数据安全防护专家。

惜亡羊之阿里云端企业代码泄露，宜补牢于自身数据安全

近日有报道称，上海一家科技公司的后端工程师历时半年，义务“为阿里云查 Bug”。他发现，阿里云代码托管平台的项目权限设置得有歧义，用户在上传代码时，可设置“private、internal 和 public”。

很多开发者以为选择“internal”，就是安全的，于是选了此选项。但是正因为此，已有包含万科、咪咕音乐、51 信用卡等 40 家企业在内的 200 多个项目代码被泄露。

工程师最初自己联系代码泄露的企业，之后开始联系阿里云客服。客服回应称，会提醒用户设置成私密项目。但是工程师发现 ,那些企业的代码 ,仍处于泄露状态。

报道出来后，阿里云官方微博已作出回应，表示：“2018 年 9 月底，我们已经增强了对 Internal 权限的中文注解，并于昨日发出全站通知提醒。同时，我们正在逐一通知之前将访问权限设为 Internal 的开发者用户，确保大家正确理解该访问权限的含义。

任何产品功能理解上的歧义，都说明我们在产品设计和用户体验上做得不够好。我们正在评估、改进相关产品设计，让所有开发者有一个更安全、清晰的使用体验。”

官方回应

截止现在，阿里云的这则声明留言不多，确都很明显帮阿里方发言：

某网友说：“这个跟平台关系不大啊。简单来说，这不是阿里云出问题，是下边的一个代码托管平台。创建项目的时候就有选择，设置错了不能怪平台吧。”

留言另一用户称：“企业内部项目设置成 private 不是基本常识吗？我从云效刚开始就使用托管平台，一直都是默认 private 的。”

那么，这究竟是阿里云的错？还是在企业上传代码的错？

其实本次泄露事件用户方及阿里云都存在失误。阿里云失误在后台中的“internal”，让学中国式英语出身的程序员们很是懵 X。并且阿里云未尽到事前提醒的义务，但是，在托管平台中上传代码的企业的程序员们，没有保证代码源头安全，才是导致代码泄露的“元凶”。

不管怎样，这次事件再次暴露了，用户对公有云的最大担心——数据安全。

企业上云，数据如何安全落地？

在上云过程中阿里云是众多企业的选择，那么，阿里云是否对得起用户的信任和买单呢？对于用户而言，阿里云品牌有保障，工作流程已然可以说规范，并且符合大多数企业需求；而对于企业的程序员来说，很多时候老板可能不懂技术，但是仅仅因为老板不懂就不好好保护代码，又怎么对得起公司的殷切期望呢？

另一方面，近年来，云厂商确实经常出现数据泄露的情况，从阿里云函数计算挂掉、直接导致国内半个互联网瘫痪、到腾讯云因为运营商光缆中断而宕机……企业是否上云，上云后的安全如何保障？成为首要解决的问题。

解决“企业上云”数据安全隐患亿赛通给出一整套解决方案，可通过数据防护，分别从文件的存储、传输、使用等方面，采用核心加密技术，巩固“企业上云”安全建设，确保在各种复杂业务场景下企业核心数据资产不被泄露和非法窃取。即保证敏感数据在加密状态下不改变和影响用户使用系统和工作效率，让安全性和可用性之间保持一定的平衡。除此之外，亿赛通针对各种敏感文件进行数据安全保护，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，确保在各种复杂业务场景下企业核心数据资产不被泄露和非法窃取。

在这个蹭吃、蹭喝、蹭 WIFI 的时代，不法分子窃取重要数据可以说是轻而易举！中国数据安全防护专家亿赛通特别提醒大家，无论个人或企业都需增强信息安全防护意识。同时，还必须加大安全技术投入，从根源防范信息泄露，从而对信息安全进行彻底保护。

【预警】春运诈骗很烧脑，防范攻略请收好 ~

这几天，朋友圈常常能看到这一幕：

“抢票了……”

“快抢啊……”

“帮忙加个速……”

“啊，没票了，明天吧！”

随着春节的临近，

抢票大战正式拉开帷幕 ~

春节想回家一趟，

真心不容易！

中国铁路总公司数据显示

2019 年春运期间，全国铁路预计发送旅客超 4 亿人次，同比增加 3176 万人次，增长 8.3%，日均发送 1033 万人次，再创历年春运新高。

此外，由于 2019 年春运开始离除夕时间较短，学生潮与返乡潮叠加，使得春运返乡车票预计比往年更为紧俏。为了能顺利回家，大家也是各出奇招，种种手段齐上阵，也没有抢到回家的车票。一直没抢到车票的乘客越来越着急，但也正是这种焦虑的心情，给了“坏人”可乘之机！

年 4 月，美国面包连锁店 Panerabread 表示，旗下网站 panerabread.com 泄露了 3700 万用户信息，而更可怕的是，在官方没有给出公告前，这种泄露信息行为已经持续了超过 8 个月。随后，安全机构 KrebsOnSecurity 表示，他们在早在 2017 年 8 月 2 日就曾发现了 Panerabread 网站的漏洞，告知对方后并没有进行及时修复，所以造成的结果就是严重的。

给大家提供几个案例，让您看清陷阱，平安回家！

案件类型

1、微商代购、网站转卖二手票

诈骗手段

不法分子在微信、微博、QQ 空间、各大二手交易网站发布虚假的代购、出售火车票信息，利用受骗市民的急切心理，骗取转账，或是登录钓鱼网站骗取银行卡信息。

案例

扬州市民王先生通过同城网，从一网友手中购买泰州至哈尔滨硬卧下铺车票，通过点击进入对方发送的链接，按提示操作后从其工商银行卡上支付 506 元。后续王先生想改签时发现无法查询到购买信息，发现被骗。

苏州市民赵先生在微信上添加一名叫“韩小红”的男子为好友，对方以能够替其买到除夕夜车票为由，让其转账 1200 元，后发现被骗。

2、虚假售票网站

诈骗手段

不法分子制作虚假购票网站，宣称保证百分之百有票，引诱受骗市民在网站上填写个人信息、银行账号、密码、验证码等，或者以交“保证金”、“加价提高抢票成功率”等名义进一步诈骗钱财。

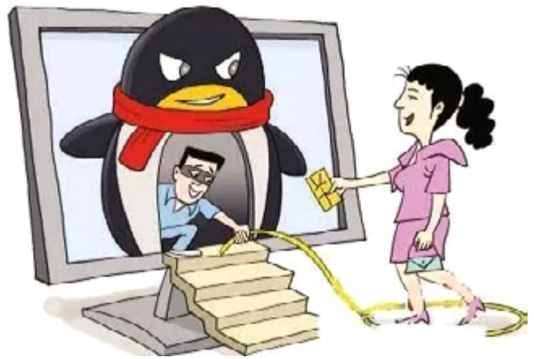
3、冒充 QQ 好友无法回国，代买机票

诈骗手段

不法分子通过获取正在国外旅游人员的 QQ 信息，冒充其身份与其 QQ 好友联系，假称在国外遇到问题无法购买回国机票，骗受害市民与“某航空公司经理”联系，代付机票钱。

案例

常州市民孙先生手机 QQ 收到一条好友验证，对方称其朋友，以在美国旅游无法购买机票为由，委托孙先生向其提供的“南航经理”购买机票，孙先生通过手机银行向对方汇款共计 20000 元，后发现被骗。



4、“抢票神器”陷阱

诈骗手段

不法分子以几元到几百元推出“抢票神器”、“抢票小工具”等软件，并且伪造好评，引诱受骗市民购买安装，待付款后才发现该软件下载链接暗含木马程序，受骗市民手机关联银行卡信息被盗用，或者是一些“网上订票流程、需知”类虚假信息，根本无法“优先抢票”

天哪！

只是想回家过年，

却没想到，

套路这么多！

春运抢票需注意四点

1、抢票软件别轻信

不法分子利用抢票高峰期人们急于买票的心理，在抢票手机软件中植入木马病毒。用户在使用软件抢票时，偷着向木马作者指定的号码发送短信，窃取用户短信记录和手机联系人信息，造成用户的隐私泄露。

2、应认准订票官网

网上订票时应认准官方网站，若一时无法判断某网站的真伪，可在该网站登录框内任意输入几个账号和密码，如均能成功登录，可基本判定为虚假网站。

3、勿点不明链接

用户使用手机通过第三方平台购票时，应通过正规第三方手机应用平台下载，不要随意点击陌生链接、扫描来历不明的二维码下载应用。在点击链接和扫描二维码过程中易造成信息泄露。

4、谨防退款设骗局

用户在购票后，要对电子客票进行必要的查询验证。一些不法分子为了掩人耳目，经常会采取“400”“800”开头的电话号码，声称是所谓的企业客服专号，要求购票者到指定网址重新填写银行卡信息或去提款机退款，此类情况均为欺诈，购票者一定要注意辨别。

春运抢票需提供乘车人真实姓名和证件信息，某些不法分子将抢票软件写入恶意代码 ,极可能导致购票者财物两空。目前国内个人隐私信息盗取、贩卖呈上升趋势。手机购票病毒样本激增，尤其是盗取用户隐私信息的病毒开始在总体数量上占据优势。同时，链接、二维码购票等移动 App 也成为泄露个人隐私信息、传播钓鱼诈骗的重要源头。亿赛通作为专业的数据安全防护专家，肩负保护企业、个人信息安全的使命，提醒大家春运抢票期间保护好个人信息，务必引起重视，千万不能让不法分子有机可乘。

亿赛通专业解决方案实现研发通讯行业智能安全管理

研发通讯行业分析

信息化时代的企业都在利用信息技术以提高企业的运营效率，致使企业百分之九十的知识产权如：程序代码、设计图纸等，都是以电子数据的形式存在企业的内部网络中。研发通讯企业在制定安全策略与具体执行这些策略的能力之间还是存在很大的差距，现存的网络安全技术大都是对外防护的问题，而且没有构筑出一个能彻底解决企业内部网络安全问题的平台，所有以电子形式存在的企业知识产权信息均有可能会以电子邮件，文件传输等形式轻而易举地流出企业。 如何才能有效的将网络安全防线，从企业网络的边缘扩展到企业所有的网络节点之上？如何预防企业内部人员的主动或非主动的泄密风险？如何从源头上保证涉密资料的安全？如何避免其他内网安全软件的各种漏洞？成为研发通讯中各个企业急需解决的重要问题。

客户需求

为提高企业内部信息管理的安全性，实现内部核心源代码存储、流转安全可控，有效防止文件的扩散和外泄，需要建立一套完善的数据保密及授权访问系统，即对于公司内部电子文档，就其使用范围、用户权限、用户操作、文件流转进行控制管理，以防止文档内部核心信息非法授权阅览、拷贝、篡改。

综上所述，为了安全和效率的平衡点，构建内网数据安全可从以下几方面防护：

1）防止内部重要电子文档被泄密；

2）防止离职或内部员工泄密；

3）数据安全系统能否支持应用的复杂性；

4）数据安全系统是否改变应用习惯；

5）数据安全系统是否改变应用流程；

6）数据安全系统是否能保障应用的安全性；

7）数据安全系统是否能支持应用系统升级。

解决方案

亿赛通数据泄露防护（DLP）系统专为企业级用户设计的数据防泄密解决方案。它不但能够对源代码、Office等进行加密保护，并且能够对加密的文件进行细分化的应用权限设置。确保企业的机密数据只能被经过授权的人，在授权的应用环境中（例如企业内部），在指定的时间内，进行指定的应用操作，并且整个过程会被详细、完整的记录下来，以便您对数据的访问记录进行安全审计。

方案价值

采用该方案后，员工保密意识大大增强，配合公司现有的保密制度，公司核心代码、设计图纸、财务报表等重要数据都得到了有力保障，业务系统的安全也得到保障，也提高了企业内部信息管理的安全性 。

部分经典客户

1、华为技术有限公司

2、神州数码信息系统有限公司

3、烽火通信

4、宇龙通信

5、天宇朗通

6、联想集团

7、晨讯科技集团

8、京东商城

9、北大方正集团有限公司

10、大连光洋科技集团有限公司

11、威海北洋电气集团股份有限公司

12、广联达软件股份有限公司

13、远光软件股份有限公司

14、郑州信大捷安信息技术股份有限公司

15、中体彩科技发展有限公司

16、华中数控股份有限公司

17、UT 斯达康通讯有限公司

18、支付宝（中国）网络技术有限公司

19、奥克斯通讯设备有限公司

20、富泓电子（香港）有限公司

……

亿赛通签约河南国网，电力能源产业又树新标杆

企业简介

国网河南省电力公司是国家电网公司的全资子公司，肩负着为全省经济社会发展提供可靠电力保障的重要任务。近年来，公司认真贯彻落实国家电网公司和河南省委、省政府决策部署，坚持推动再电气化，构建能源互联网，以清洁和绿色方式满足电力需求。作为全球能源服务国计民生的先行者，获得全国模范劳动关系和谐企业、国家电网公司文明单位和省级文明单位等荣誉称号。

需求背景

保密工作是党和国家的一项重要工作，国家电网公司作为社会、经济的重要保障 ,其对保密工作有着更高的要求。为认真贯彻国家电网公司保密工作要求，着力消除泄密风险隐患，为进一步提升保密工作整体水平，亿赛通以专业的服务水准和技术能力深获用户认可，最终力压众多业内多家企业以高价中标，与国家电网河南省公司携手构建省级电网企业保密管理体系，实现了公司在能源领域的重大突破。

解决方案：

（1）智能识别文件内容：利用机器学习、自然语言识别、数据指纹等智能识别技术，识别文件内容，提高敏感信息识别精度。

（2）传输途径全面控制：对内网邮件、即时通讯、网络共享、FTP 等网络传输途径，U 盘拷贝、打印等终端传输途径，根据风险等级采取相应控制措施，及时阻断风险信息传播途径。

（3）文件自动授权控制：与内网邮件、即时通讯进行深度集成，实现敏感文件自动授权密文传输，防止文件越权查阅。

（4）屏幕文件水印控制：具备屏幕水印和打印水印功能，可对打印者信息进行追溯，有效防范屏幕拍照、文件打印造成的失泄密风险。

（5）强化风险动态监控：实时审计用户操作行为，生成敏感信息全生命周期日志记录，动态绘制风险热点地图 ,为评估失泄密风险防控重点提供精准数据支撑。

项目成果：

亿赛通为河南省国网提供了完善的数据安全智能管理平台（DSIP）解决方案，建立了一套数据安全防护体系，有效地保障了各个环节数据的安全运行，避免了公司敏感数据遭窃的风险，提高数据安全的智能化管理，为河南省国网打造了一个良好的信息安全办公环境。