



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



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

4-10 国内行业新闻

11-13 国外行业新闻

14-19 2017 年最严重的七大数据泄露事件

亿赛通动态 ESAFENET NEWS

20/21 技术荣耀 | 创新铸就未来 亿赛通荣获 2017 年度最佳技术创新奖

22/23 亿赛通以“人”铸造企业核心要素，荣获“先进企业”和“先进基层工会”双项荣誉

24-27 披荆斩棘，砥砺前行，亿赛通 15 周年新春年会开启 2018 年新篇章

亿赛通小贴士 ESAFENET PROMPT

28-30 常用手机 APP 被质疑存在风险，防范信息泄露不能放松！

31 离职员工联合公司内鬼非法窃取数据，亿赛通防内鬼有妙招！

32/33 春运抢票作战开启，谨慎“抢票陷阱”！

34/35 网盘分享文件 = 隐私泄露？有亿赛通数据安全卫士来帮你

36/37 答对 12 题就能“一夜暴富”？当心隐私泄露！

典型案例 TYPICAL CASES

38/39 党政军数据安全综合解决方案及案例

感谢有你一路相伴

15 年的并肩携手
奋斗的汗水刚刚拭去
15 年的患难与共
胜利的笑容正在蔓延

感谢一直以来陪伴亿赛通的你们
让我们继续携手共进
拥有新的一切，新的开始
共创新的未来

1、个人信息安全规范国标将引导企业自律



“保护” 新华社发 程硕 作

摘要：由全国信息安全标准化技术委员会制定和归口管理的个人信息保护国家标准《信息安全技术 个人信息安全规范》于日前正式发布，内容涵盖个人信息的收集、保存、使用、共享转让以及安全事件处置等方方面面。该《规范》将于 2018 年 5 月 1 日开始实施。

2、上百个 GPS 定位服务被曝漏洞，用户信息面临暴露风险



摘要：互联网汽车安全问题又一次爆发！两名研究人员披露，上百款 GPS 和定位跟踪服务因使用简单易猜的默认密码 (123456) 和开放式 API 接口，导致其位置跟踪设备记录的位置等信息存在暴露风险。

3、河南 47 家金融机构被罚 716 万元：瞒报数据、泄露信息



摘要：中国人民银行郑州中心支行向社会公布的行政处罚信息显示，自 2017 年 11 月 6 日至 12 月底不到两个月的时间内，因涉及瞒报虚报数据、过失泄露信息等违规行为，河南辖内 47 家金融机构受到行政处罚，罚款金额达 716 万元。

被处罚的违规机构涵盖各类金融机构，既包括四大国有银行，民生、光大、广发、中信、浦发等 5 家全国股份制银行，也包括 21 家地方农商行和农信社、7 家村镇银行以及中原银行、平顶山银行等 2 家城商行；同时还包括 6 家保险公司、1 家资产管理公司和 1 家涉及金融服务的网络科技公司，共计 47 家。

4、在泄露数百万用户数据后 玩具制造商伟易达被 FTC 处以 65 万美元罚款

摘要：据外媒报道，2015 年智能玩具制造商伟易达 (VTech) 的安全漏洞导致数百万家长和孩子数据遭曝光。日前美国联邦贸易委员会 (FTC) 宣布对其处以 65 万美元的罚款。



5、去年公安机关侦破侵犯公民个人信息案件 4900 余起



摘要：据统计，截至 2017 年 12 月 20 日，全国公安机关当年累计侦破侵犯公民个人信息案件 4911 起，抓获犯罪嫌疑人 15463 名，打掉涉案公司 164 个。

6、中国网络黑色、灰色产业年产值达千亿 保护信息安全刻不容缓

摘要：由中国信息通信研究院牵头编写的《中国企业数据保护白皮书》12 日在京发布。报告显示，目前中国网络黑色和灰色产业的年产值已达千亿，而网络安全的产值不到 300 亿。



7、涉嫌侵犯用户隐私 工信部约谈 百度、支付宝、今日头条



摘要：11 日，针对近期媒体报道相关手机应用软件存在侵犯用户个人隐私的问题，工信部信息通信管理局约谈了百度、支付宝、今日头条。

8、整形医院客户信息遭泄露 客户接二连三被“劫”走



摘要：近日，武汉一家整形医院发现，他们的客户信息遭到泄露，预约好的客户接二连三被“劫”走，让医院蒙受了巨大损失。到底是谁窃取了这些商业机密？

9、2018 年，越来越多医疗行业成为勒索软件攻击目标



摘要：医疗行业似乎已经成为全球网络犯罪分子获取丰厚利润的攻击目标，在已经过去的 2017 年以及已经到来的 2018 年，越来越多的医疗中心和医院发生了恶意软件攻击事件。

10、非法下载新生婴儿数据 50 余万条，四川警方揪出卫计系统内鬼

摘要：成都市“妇幼信息某管理系统”市级权限账号密码，多次将 2016 年至 2017 年的成都市新生婴儿信息及预产信息导出后，通过线下交易方式，将其信息出售。累计非法下载新生婴儿数据 50 余万条，贩卖新生婴儿信息数万条。

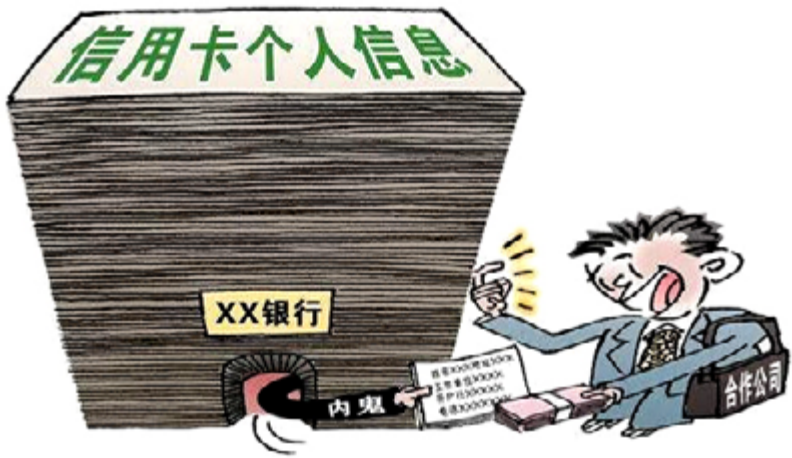


11、窃取学生信息 500 余万条 “黑客”被绵阳警方跨省抓获



摘要：张某利用黑客工具和技术曾多次入侵四川省教育部门学籍系统，窃取 500 万余条在校学生和家长信息后贩卖牟利，同时网安民警查获张某用于作案的大量黑客软件和其他公民隐私类信息多达 1T。

12、7 家机构窃取倒卖个人信用信息 新疆人民银行系统开出 192 万元罚单



摘要：1 月 18 日，记者从中国人民银行乌鲁木齐中心支行了解到，2017 年，新疆人民银行系统将违规查询、信用信息泄漏作为新疆征信市场监管领域的重点，对 7 家机构及相关管理人员给予行政处罚 192 万元。

13、山西：泄露个人信息，最高罚款 50 万.....



摘要：个人信息被泄露，网络运营者应该承担怎样的责任？1月17日，省政府发布《山西省公安机关网络安全管理行政处罚裁量基准（试行）》对未按照网络安全制度的行为做出了裁量基准。

14、广东“安网 2017” 侦破案件 4588 起
缴获被泄露的公民个人信息 7.1 亿条

摘要：广东省公安厅召开发布会，通报严打整治网络犯罪“安网 2017”专项行动全年的战果以及“安网 2018”专项行动计划，并公布了 2017 年度广东公安十大精品网络案件，其中多个案件创造全国第一，比如打掉网络攻击“黑产圈”排行第一的犯罪团伙“暗夜攻击小组”。此外，首次以《白皮书》形式发布移动 APP 监测情况和安全状况。



1、美国国土安全部数据泄露
24 万员工个人身份信息



摘要：美国国土安全部 (DHS) 周三证实，该机构发生个人信息数据泄露，涉及 24 万多名现任和前任 DHS 员工的个人身份信息。该机构称，泄露的国土安全部员工个人信息包括姓名、社会安全号码、出生日期、职位、级别和工作地点等。

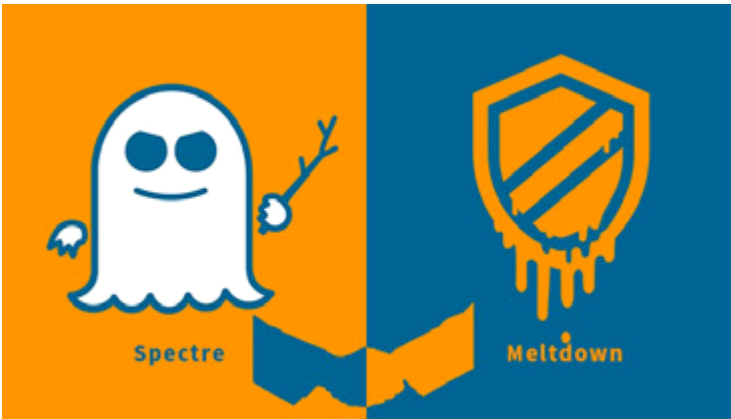
2、印度全民个人信息遭泄漏 售价不足 6 英镑

摘要：根据印度《论坛报》(Tribune) 进行的调查显示，超过 10 亿印度公民的个人资料（包括指纹和虹膜等生物识别信息）正在在线出售，售价不足 6 英镑。这些数据是存储在世界上最大的国营生物识别数据库——Aadhaar 中，该数据库除了收集印度公民的基本信息（名字、照片等）外，还存有被记录者的指纹、虹膜及其他生物识别信息。



3、我们怎么办？英特尔 CPU 漏洞事件全面解析

摘要：作为 2018 年的首个大新闻，这次被曝出的芯片级漏洞波及范围之广、程度之深是我们始料未及的。而位于漩涡的中心：Intel 扮演的的是一个相当重要但尴尬的角色。

The image shows two logos side-by-side. On the left is the 'Spectre' logo, which features a white ghost-like figure with a single eye and a small branch-like appendage, set against an orange background. Below it is the word 'Spectre' in white. On the right is the 'Meltdown' logo, which features a yellow shield with a diagonal crack and a small figure at the base, set against a blue background. Below it is the word 'Meltdown' in yellow.

4、IBM：去年金融业数据泄露逾 2 亿条



摘要：IBM X-Force 团队发布 IBM X-Force 威胁情报指数显示，2016 年，金融服务业遭遇的网络攻击规模远超其他任何行业，高出所有行业平均水平 65%。指数显示，2016 年金融服务业数据泄露逾 2 亿条，较 2015 年猛涨 937%。不过，受益于安全措施的投资，该行业的数据记录泄露数量在所有行业中仅排名第三。研究称，2016 年，网络罪犯对金融业的攻击出现大幅复苏，与企业 and 客户数据相关的金融收益引发了网络罪犯的兴趣，金融机构被迫抵御攻击的数量较 2015 年增长了 29%。

5、特朗普政府首份《国家安全战略》曝网络安全缺陷



摘要：美国白宫于 2017 年 12 月 18 日发布了特朗普任内首份《国家安全战略》报告。这份长达 68 页的报告将“保护国土安全”“促进美国繁荣”“以实力维护和平”以及“提升美国影响”列为国家安全战略的“四大支柱”，并强调本届美国政府在全球及外交政策层面将始终坚持“美国优先”的方针政策。该报告还囊括了用于改善美国国家网络安全方法的行动纲要清单。这份长达 68 页的《国家安全战略》报告囊括了用于改善美国国家网络安全方法的行动纲要清单，但这份特朗普任内的首份报告却遭到多方质疑。

6、加拿大男子收集了超过 30 亿 泄露数据 非法盈利 24 万多美元



摘要：加拿大皇家骑警今天宣布，他们已经起诉了一名名叫乔丹的 27 岁男子，是他运营了 LeakedSource.com，该网站收集了超过 30 亿数据泄露事件中的数据，其中包含大量明文密码，并以此非法盈利 24 万 7 千美元左右。

2017 年最严重的七大数据泄露事件



如果新闻中经常出现“泄漏”、“泄露数据”和“漏洞”这些词，那就不仅仅是你自己了。重大数据泄露的频率正在增加，根据个人信息失窃资源中心统计，预计 2017 泄露事件将超过 1500 起。这比 2016 年度增长了 37%，而且今年本身就是个人信息泄露的最高纪录年。

尽管大多数数据泄露都是小规模和可控的，但今年出现了少数严重的安全事故。以下是 2017 年度最大规模的数据被盗和数据泄露事件。

1、Equifax



Equifax，美国四大信用报告机构之一。Equifax 在 9 月份透露，网络犯罪分子已经渗透到他们的网络中。漏洞泄露了一亿四千三百万美国人的数据，基本上包括了美国的每一个成年人。泄露的信息包括姓名、社会保险号码、生日、地址，在某些情况下还包括驾照号码。

更糟糕的是，约 209000 名消费者的信用卡号码和

182000 人的信用报告纠纷相关文件也被曝光。作为回应，Equifax 为所有的美国人提供一套身份盗窃保护服务，不管他们是否受到了影响。这些服务包括高达一百万美元的身份盗窃保险和社会保险号码监控，对 2018 年 1 月 31 日之前注册的任何人都是免费的。（虽然我们怀疑这些身份盗窃保护服务的有效性，并不推荐别人购买。）

2、Uber



这一数据泄露实际上发生在 2016。但由于 Ube 之前的普遍不光彩，我们直到今年 11 月才知道这件事。已泄露的数据包括五千万名优步客户的姓名、电子邮件地址和电话号码。大约七百万名司机的个人资料也被曝光，其中包括大约 600000 个驾照号码。

黑客首先访问了 Uber 工程师使用的一个私人 GitHub 网站，从而成功地窃取了数据。从那里，他们获

得了 Uber 的 AMS（亚马逊云计算平台服务）登录凭据，并访问了个人数据。然后黑客利用这些数据敲诈 Uber。为了掩盖这起事件，优步高管向黑客支付了 100000 美元，用于删除数据并保持沉默。这起事件是在 Uber 新任 CEO Dara Khosrowshahi 发现并向监管部门报告后才被曝光的。在一篇博文中，Khosrowshahi 说：“这一切都不应该发生，我也不会找借口。”

3、Edmodo

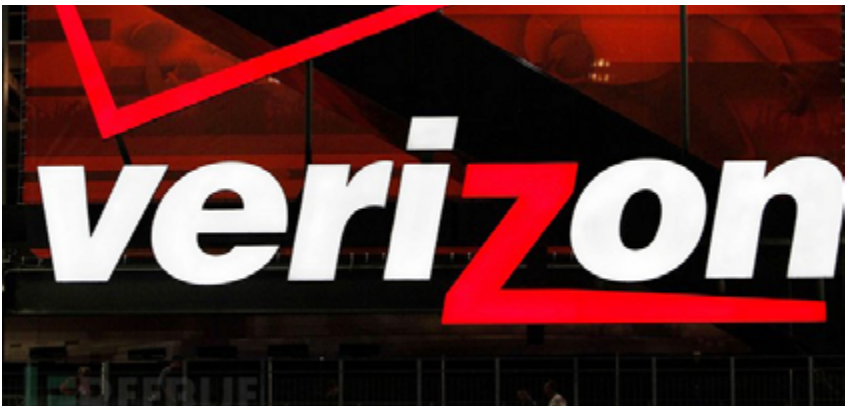


不是只有成年人才会把他们的信息泄露出去。五月份，Motherboard 公司报告称，社会学习平台 Edmodo 被黑了，该服务由教育工作者和学生使用，大约有七千八百万用户，一名名为“ncly”的黑客声称，他获得了其中

七千七百万人的账户数据。

这些数据是在黑暗网络上出售的，但是很明显，一个主要用来分配作业和创建课程计划的网站的帐户并不是特别有价值的。黑客将整个数据库的价格定在略高于 1000 美元。

4、Verizon



您是否在 2017 年前六个月致电过 Verizon 客户服务？那么你的数据可能就在无意中暴露出来了。

ZDNet 报告称，总部位于以色列的 Nice Systems 公司未能确保一个 Amazon S3 存储服务器的安全，里面包含一千四百万 Verizon 客户记录，导致客户姓名、手机号码和帐户 PIN 均被泄露。

幸运的是，Verizon 能够在其他人访问数据之前保护数据。在 CNBC 一份声明中，Verizon 发言人说“我们已经证实，除了 Verizon 或其供应商之外，只有一位研究员才能进入云存储区，他让我们注意到了这个问题。换句话说，Verizon 或者 Verizon 的客户信息没有丢失或被盗。”

5、Deep Root Analytics



数据分析公司 Deep Root Analytics 是由共和党全国委员会承包的，它披露了一亿九千八百万名公民的公开数据。这意味着每三个美国人中就有两个受到影响。公开的信息包括姓名、生日、电话号码，以及最令人不安的选民登记细节。

这个漏洞是由安全研究员 Chris Vickery 在 6 月 12 日发现。他的分析显示，该公司的数据库存储在亚马逊的云服务器上，没有密码保护，时间大约有两周。任何人都有能力下载这 1.1TB 的数据。

6、SONIC 汽车快餐店



数百万名只想点芝士汉堡和奶昔的顾客可能无意中把他们的信用卡信息给了小偷。快餐连锁店 Sonic 承认，餐厅的支付系统数目不详，客户的信用卡信息也遭到了破坏。安全研究员 Brian Krebs 发现被盗的信用卡号码流入了地下市场，网络罪犯在那里买卖敏感的金融数据。

7、所有的 WiFi 设备



2017，我们还发现，从本质上讲，通过 WiFi 网络传输的所有数据都是脆弱的。计算机科学家 Mathy Vanhoef 宣布 WPA 2 加密协议中的漏洞使 WiFi 网络无需登录凭据即可访问。黑客们可以通过利用密钥重装攻击（KRACK）来访问 WiFi 数据。目前还不清楚是否使用这种方法窃取了任何数据，但该漏洞自 WiFi 开始以来就一直存在。

幸运的是，在发现问题后不久，各大科技公司就开始

发布补丁。本月初苹果公司为所有的 iPhone 修复了这个安全漏洞。一些路由器制造商已经发布了最新的固件，以防止 KRACK 攻击。

数据泄露的数量或者规模都在不断上涨，这表明我们所面临的风险正在超过企业采取安全措施的保护能力。除非公司能够改善其安全态势，否则防止数据泄露造成严重损害的责任将落在个人身上。

技术荣耀 | 创新铸就未来 亿赛通荣获 2017 年度最佳技术创新奖



今日重磅 亿赛通再获 2017 年度最佳技术创新奖

第十二届中国企业 “IT 印象•新 IT，新价值” 年终评选活动已于日前揭开谜底。该活动由工业和信息化部中国电子产业发展研究院指导、51CTO 主办。整个评选活动秉承着公平、公正、公开的原则，从品牌、产品、解决方案、应用服务等角度对企业“技术、成就、创新”以及对产业的支持和服务进行调查。通过媒体曝光度、微信微博曝光、编辑推荐等方式对 2017 年的中国企业级 IT 应用与创新成就进行总结。最终，亿赛通凭借领先的科技创新技术与研发实力，以及在数据安全领域中的突出地位，经过激烈的角逐荣获应用服务类 2017 年度中国数据安全最佳技术创新奖。

实力铸就品牌，科技创新未来

亿赛通成立十五周年，在整个数据安全领域市场经营成熟，所研发的数据安全产品广受客户的认同。2017 年 8 月，亿赛通更是重磅发布数据安全智能综合管理平台（DSIP）和第一款个人版“数据安全卫士”，产品已全面投入及使用到千万家客户，再一次向业界展示企业拥有的一流技术和一流服务。



作为高新技术企业，亿赛通从未停止创新，一直走在科技前沿的探索之路，为此企业不断加大研发力度，不断提高公司硬实力，为广大客户提供最具前沿化、最具科技化、最佳化的数据安全产品和解决方案，在坚持发扬“创新”的精神理念下，在行业中创立了一个又一个新的里程碑，从而促使亿赛通更加坚定的向前冲进。也正是亿赛通坚持不懈的探索精神、创新成果和市场的广泛赞许，让亿赛通在本次评选活动当仁不让拿下“最佳技术创新”奖项。



2018 亿赛通将会继续怀着初心，一路前行，做数据安全行业的佼佼者，做中国数据安全的防护专家。

亿赛通以“人”铸造企业核心要素，荣获“先进企业”和“先进基层工会”双项荣誉

近日，由中关村科技园区海淀园工会工作委员会发起举办的2017年度海淀园“双爱双评”评选活动已圆满落幕。经审核，中国数据安全防护专家——亿赛通荣获“先进企业”和“先进基层工会”双项荣誉。

2017年度，中关村海淀园工会紧紧围绕海淀园工委和上级工会明确新使命、新任务的指导意见，活动围绕核心区“减人、添秤、服务”重点工作，找准工会工作的切入点、着力点和落脚点，不断强化工会职能，树立工会组织良好形象，优化创业创新环境，开展2017年度海淀园“双爱双评”评选。该活动已连续举办超过十年，为激发创新资源活力，打造具有全球影响力的科技创新中心新地标不懈努力，是园区内最具影响力的评选之一。



亿赛通从创立之初，一直坚持以员工的福利为核心要素，在这一路的坚持中，很荣幸在2017年度，能够在众多企业中脱颖而出，被中关村科技园区海淀园工会工作委员会评选为2017年度海淀园“双爱双评”活动“先进企业”和“先进基层工会”两项荣誉奖项。多年来，亿赛通在保障员工的经济利益、民主权利和满足职工的精神文化需求方面做出不懈努力。2017年，曾在各大重要节日为员工发放节日礼品，也送去了工会组织的温暖。亿赛通工会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。



亿赛通稳居数据安全行业领衔地位，带领行业走向科技前沿，打造行业标杆形象，之所以能够取得如此优秀的成果，首先是因为内部制度完善正规，着实确保公司所有工作人员的利益，并且随着企业的发展不断得到改善。其次，企业文化始终秉持“服务客户、持续创新、永担责任、专业至上”的核心价值观，使得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。

披荆斩棘，砥砺前行，亿赛通 15 周年 新春年会开启 2018 年新篇章



在大家的翘首期盼下
一年一度的亿赛通年会盛典
于 2 月 7 日盛大举办
在朋友圈被年会刷屏的日子里
亿赛通的年会又有哪些不同呢？
睁大你的眼睛
带你领略
不一样的年会风景！

2018 “感谢有你”暨亿赛通15周年新春年会



开场篇

年会现场总结 2017 年战果
部署并展望 2018 年
希望 2018 年能再创辉煌
年会就此拉开序幕



优秀团队

颁奖篇

年会是收获的季节
是对员工全年辛苦工作的肯定
在 2017 年的辛勤工作中
涌现一大批优秀个人及优秀集体
特在年会中进行表彰



优秀个人



五年贡献奖

五年贡献奖

五年，这个时间让执着彰显价值
对价值观的认同
对事业的热爱
对公司的认可
让他们与亿赛通风雨同舟、相濡以沫、共同成长



十年贡献奖

十年如一日
他们与企业同风雨、共命运
用不懈的努力为企业创造着一笔笔财富

节目篇

我们有
最活力的开场舞表演



最热情的歌曲演唱

抽奖篇

说到年会万众期待的部分
一定是当天最激动人心的“红包雨”环节
“现金红包”统统抱回家!!!



最专业的二胡、小品



15 年的并肩携手
奋斗的汗水刚刚拭去
15 年的患难与共
胜利的笑容正在蔓延
感谢一直以来陪伴亿赛通的你们
让我们继续携手共进
拥有新的一切，新的开始，
共创新的未来

常用手机 APP 被质疑存在风险， 防范信息泄露不能放松！



2018 年悄然而至，17 年发生的信息泄漏事件现在回想起依旧让人心惊胆战，18 年我们希望可以风平浪静。可惜事与愿违，刚刚开年，信息泄露事件频发，现在就跟小编一起回顾近期发生的泄露事件吧。

爆料篇

1 “跳一跳”靠外挂“霸榜”

近期，微信小游戏“跳一跳”火爆网络，该游戏用户日活跃量超过 1 亿，远高于同期“王者荣耀”和“绝地求生”两款游戏的微信指数。这款游戏简单易上手，但想拿高分却很难。为提高排名，网上出现了高分攻略以及代练服务和外挂软件。有安全专家提醒，当心外挂和代练有风险，可能泄露个人信息。由于授权代练需登录自己的微信号，极易造成个人隐私泄露，对方甚至可能利用用户的微信号传播其他诈骗信息，影响亲朋好友。



2、旧手机泄露隐私机密

近年来，手机更新换代速度越来越快，智能手机用户平均约 17 个月就更换一次手机，旧手机的处理方式也成为关乎隐私安全的重要问题。如果旧手机落入犯罪分子手中，通过技术手段对信息加以恢复，手机的原主人将面临照片、视频等隐私被曝光，短信、通讯录、微信、QQ 被用来诈骗，网银或第三方支付软件被盗刷，邮件等商业机密被窃取等问题。



3、12306 过度获取用户隐私

12306 作为全国唯一一个官方网路购票渠道，每逢买票都不得不使用它。近日，某网友订票时就发现，12306 手机客户端弹出了一则提醒，指出它可能会获取用户的位置信息、相机相册、文件存储和电话等个人信息。网友吐槽“你只能同意，不同意就进不了页面，订不了车票。”其实，在 Android 端，手机应用过度获取用户隐私已是普遍现象，获取位置信息、读取手机号、打开摄像头、使用话筒录音.....这些手机应用经常会提出的请求，全部涉及用户的隐私权限。



分析篇

信息会造成有些是故意，有些是无意；有些是泄露他人隐私，有些是泄露自己隐私。隐私泄露的原因主要是：受利益驱动。

注意事项：

- 1、小游戏、春运抢票都变成了不法分子盗取用户隐私信息的渠道。充分利用了用户寻求高分、回家过节的迫切心情，轻而易举获得了用户的信息。
- 2、数据时代，信息就是资源，一些不法人员借助网络的虚拟性与快速传播性来贩卖数据，从而获取利润，造成了用户信息大量泄漏。
- 3、个人或者团体利用隐私信息能满足普通受众的“窥私”心理，贩卖隐私信息，博取眼球，制造轰动效果，获得利润。



提醒篇

中国数据安全防护专家亿赛通提醒广大网友，一般而言，为保障用户的信息安全，谨慎同意 APP 获取用户信息，游戏禁止使用外挂或代打，以防个人身份信息外泄。在出售或折旧旧手机的过程中，防止个人照片、电话本等私密信息被盗。网友要时刻加强自身隐私保护意识，以防带来不必要的个人损失。

离职员工联合公司内鬼非法窃取数据，亿赛通防内鬼有妙招！

近日，警方破获一场大型小区住户购房信息泄露事件
全市 70 个小区，至少 1 万 3 千多住户信息都遭泄露
随便什么人，花 1 毛 5 分就能买到你的隐私
细思恐极！触目惊心！心有余悸

事件经过

王某频繁接到装修公司和家具店老板的电话
怀疑自己的信息被别人恶意透露，就到派出所报了警
公安局十分重视此案
特派网警大队与派出所联合侦办
通过警方侦查，民警找准这些推销电话的出处
位于市区某酒店，派出所随即派民警
到该宾馆进行蹲点抓捕。

如何犯罪

民警在现场发现，十几个推销员聚集在一起，
每人手里都有一份客户信息，
包括姓名、电话号码、小区房号
有的还包括身份证号码，推销员在客户的个人信息旁边还
写着“已打”、“挂断”等标注
电脑里查到了更多各大楼盘业主个人的购房信息
其中涵盖 70 多个小区，数量多达 13000 余条

房地产公司有“内鬼”

杨某之前在某房地产公司任职
离职后主动联系房地产公司的项目经理陈某
朋友开了一家中介公司
想要一些客户资料，用来打开市场
在利益的驱使下
陈某利用职务便利，以非法获利为目的
将自己掌握的业主的个人公民信息

提供给了嫌疑人杨某
杨某将从陈某处非法获得的公民信息
转卖给装修公司、家具公司等，从中非法获利
有图有真相哦！



小贴士

如何防止内鬼？亿赛通为你出妙招

看完这个事件，不少 BOSS 要开始注重自己公司的数据安全了，不仅仅要防外，防内更加重要哦。各位 BOSS 也请放心，在这里“小亿”会与您共同防内鬼、消外患，全方位保障您的数据安全。亿赛通针对竞争对手窃密、员工离职拷贝、内部有意无意泄密、间谍 / 黑客窃密、设备丢失、非法脱机、电脑报废数据丢失等等的状况下，所研发的产品以数据加密技术为核心，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。

亿赛通作为中国数据安全防护专家，15 年来一直致力于数据安全行业，防护产品深入各个行业，赢得客户广泛的信赖，并与客户取得长期合作的关系，为其保障企业数据资产安全无风险。

春运抢票作战开启， 谨慎“抢票陷阱”！



2018 年春运抢票作战已经打响，旅客可以通过网络、电话预定 2018 年春运期间火车票。2018 年开始，90 后已全部成年，逐渐成为外出务工的主力。作为在互联网发展下成长的一代，90 后更倾向于使用更便利、更智能的第三方抢票平台，在提高抢票成功率的同时，能抢到更舒适称心的火车票。也正是因为这样的原因，越来越多诈骗分子将魔爪伸向 90 后群体。每年春运期间，都有不法分子利用旅客回家心切心理，借助购票、退款等多种形式设下陷阱实施诈骗。

陷阱一：抢票软件嵌入病毒，泄露用户隐私

春运放票期间，除了 12306 官方抢票软件，很多用户都选择用第三方抢票软件购票，这就给不法分子以可乘之机，他们往往推出载有病毒的抢票软件，意在窃取用户个人信息及钱财。用户一旦使用带有病毒的抢票软件，不法分子将未经同意给用户发送垃圾短信、消耗资费，更有甚者可因此获知用户个人信息。



陷阱二：假客服通知有余票，非法链接设埋伏

与网购退款诈骗、航班延误取消短信一样，乘客网购火车票后也很可能遭遇电话或短信诈骗。由于很多第三方抢票软件都有自动刷票功能，用户很可能接到各种各样的余票通知，这些通知往往带有抢票链接，用户无法分辨此链接是否为钓鱼链接，如果盲目点击这些链接，就很可能中招。



陷阱三：钓鱼网站伪装抢票网站，骗取信息和钱财

春运火车票开售，电脑网页和手机客户端往往充斥着打着“春运火车票代抢”“帮购票”等名头的信息，用户点击后会进入所谓的代购网站。这些网站乍看起来十分正规，实则是通过网页模板的方式，伪装成“票务代购点”的钓鱼网站，内置木马可能窃取用户的信息。

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。手机购票病毒样本已激增到近 7000 个，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，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，肩负国家数据安全、企业数据安全、个人数据安全的保护使命，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。

网盘分享文件 = 隐私泄露？ 有亿赛通数据安全卫士来帮你

小爆料一

某网盘泄露用户个人资料

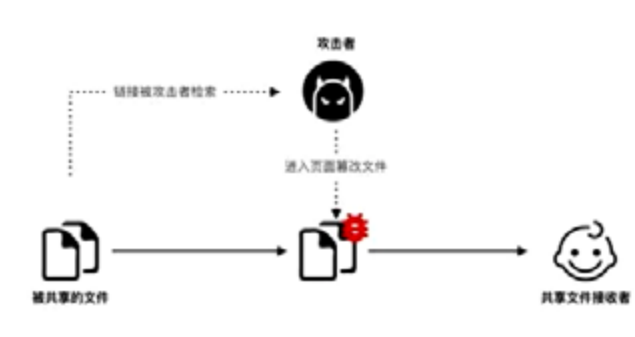
近日，有网友爆料称，很多用户因误操作主动在某网盘上分享内容，上万条车主个人信息，企业、政府高官信息和各种数据库都被泄露。文章指出，该网盘用户在使用“分享”功能时，因误操作主动分享隐私的照片、文件，同时没有加密，导致分享的内容出现在用户的主页上，还能被所有人通过第三方网站搜索看到。这意味着，所有该网盘用户只要上传了自己的照片并公开分享，只要有人想找私人网盘上的照片，基本都能找到。



小爆料二

某在线数据管理网站共享存在风险

某知名在线数据管理网站被发现其文件共享机制存在安全风险，导致许多企业的部分机密数据和文件可以被谷歌、必应等搜索引擎直接检索。该网站在处理云存储账户上存在缺陷，导致一个简单的搜索引擎查询就可以让企业或个人的机密文件被任何人访问。攻击者利用该问题可以访问企业存储在“云协作”上的数据，该企业网盘在国外相当出名，在中国也拥有一定的用户，它除了提供常见的文件存储、同步功能之外，还提供了一项用于多人共享文件和数据的“云协作”功能，而问题正是出在这一功能上。



小爆料三

网盘泄露影视样片，储存存在风险

热播电视剧《欢乐颂 2》在播放期间，样片在某知名网盘被泄露，众多网友都提前观看到“大结局”。其实这已经不是第一次发生网盘泄露送审样片事件，之前的《人民的名义》、《三生三世十里桃花》、《最好的我们》、《芈月传》都曾发生过泄露，可见，网盘现在是个重灾区，存储文件、照片并不安全，随时都有可能造成资源外泄。



要想防止网盘泄露，可以使用“亿赛通数据安全卫士”，对个人 PC 端的重要信息或核心资料在进行全面防护的个人版安全产品。即当您在将个人的重要文件、照片上传到网盘之前，将文件进行加密保护，从根源保护文件才是最重要的。不法分子企图盗取您电脑中的重要文件时，接收者打开文件首先需要进行身份认证，方可阅读，可以有效的防止重要信息在存储中，以及外发、传输给第三方时被有意或无意非法扩散或二次使用，这样就可安心上传到网盘。老铁，总有需要你倾心呵护的秘密资料，交给亿赛通数据安全卫士帮你守住秘密吧！

亿赛通送福利喽！！



各位小伙伴们，现在关注“亿赛通”微信公众号，回复“激活码”，我们会为大家推出“数据安全卫士”验证码，免费使用一年哦，领取后的小伙伴，就可以为您的敏感资料安全保驾护航啦！

答对 12 题就能 “一夜暴富” ？ 当心隐私泄露！



毫无征兆地，直播答题迅速掀起一股热潮，成为互联网行业 2018 年首个现象级事件。不少平台纷纷推出答题软件和答题节目，并通过疯狂“烧钱”吸引用户参与。玩家阵营也不断在壮大中。如今，已有很多网友热衷在线直播答题游戏。在奖金的诱惑下，许多人开始借助人工智能外挂答题。今天，我们就来说说直播答题风靡全国后所引起安全问题。

复活币网上生意火爆

由于直播答题没有门槛，而且有复活机制，所以参与者众多。不过，尽管有复活玩法，但很多用户已经把手里的复活卡用没了。某电商平台，输入关键词“复活币”，跳出来数十家经营“复活币”的卖家。“复活币”按照答题平台的不同，价钱在 0.5 元至 2 元 / 个不等，排名前几的店铺，每日销售额都在千元以上。玩家需要给出自己的邀请码，卖家就会找人刷币，

不过由于需求火爆，不少店家都表示单次购买有上限，此外不接急单。不过也有店家表示，玩家想要立刻拿复活币，需要加价，买得越多加价越高。



答题催生外挂产业

日前网上各种所谓的“交流群”、“答题群”广告满天飞。随便点开一个“答题群”，加入一个 QQ 群，客服表示有“辅助软件”可以出售，保证能答对 3 ~ 4 道题，且答题成绩非常好，只需要 30 元。“前几天卖到 50 元，这几天需求量大，我们降价有优惠。”在各个 QQ 答题群中，还有人售卖第三方软件，软件可以在手机屏幕上一分为二，上面一部分是答题界面，下面一部分是百度检索界面，每次主持人出题后，搜索栏会变成该题目，并使用屏幕拍照答题界面的题目，在百度自动搜索相关信息。



信息泄露得不偿失

以往的经验告诉我们，靠刷复活币、用答题外挂秒变答题高手肯定会付出代价！刷复活币、使用外挂的后遗症已经慢慢揭露：据网友爆料，这些作弊神器需要玩家提供账号信息，不法分子由此获得网友的个人信息。另有网友表示，使用外挂后，手机出现 BUG。与此同时，答题活动体现需要提交身份证号码、银行账户等非常敏感的个人信息。一旦这些信息泄露，将会给用户的财产甚至人身安全带来很大隐患。而且，不排除个别企业推出直播答题活动的目的是为了迅速收集大量用户的个人信息，进而借此用于牟利。



亿赛通作为专业的数据安全防护专家，在此提醒广大网友，直播答题游戏本意是把知识和娱乐相结合，实现了知识的趣味普及，既丰富知识，也有挑战性。而依靠答题神器答题则失去了它本身的挑战性和趣味性。如果一味靠作弊答题、瓜分奖金致富的想法并不可取。而且还要承担警惕个人信息泄露风险的风险，仅仅是为了一点点的奖金，得不偿失！

党政军数据安全综合解决方案

一、行业分析

随着信息化建设的不断深入，信息系统的安全性已经成为政府、军工行业必须面对的一个重要问题。面对当今世界日趋复杂的区域军事斗争及和平演变局势，利用高科技对军队及军工科研单位实行信息化管理，快速增强军队应对各类突发事件综合实力的同时，因所涉及的硬盘数据种类多、层面广、涉密度高，军工各级部门所承受的数据安全保密压力也与日剧增。

军工企业保密资格认证要求军工企业的涉密网络必须由具备涉密系统建设资质的单位进行设计和建设，遵循的技术规范为 BMZ1-2000《涉及国家秘密的计算机系统保密技术要求》、BMZ2-2001《涉及国家秘密的计算机信息系统安全保密方案设计指南》。其中明确提出涉密网络必须具备以下技术措施：备份与恢复、病毒防范、身份鉴别、访问控制、信息加密、数据加密、安全审计、入侵监控等。

军事机密泄密

军队作战部队的作战计划及相关大量文档，因人员操作失误或硬盘损伤不慎丢失，难以恢复，不仅以往心血付

之东流，丢失内容所涉及的兵力部署、军队实力、作战装备等国防军事机密也极有可能泄密，为国家带来重大损失和外部军事威胁。

军事科研成果遗失

军工企业在重大军事科研项目和技术创新领域的研发攻关成果损坏遗失。此类数据在安全性和涉密性上均有严格要求，国家相关部门为防止泄漏，不允许对其中绝密数据进行备份处理。一旦数据丢失将会造成关键技术和研发计划的严重脱节，导致国家军工设计研发成果、安全信息的彻底流失，给国家带来难以估量的损失。

二、客户需求

当下，黑客针对政府、军工单位攻击呈现攻击主体组织化、目标趋利化、政治化；手段智能化、网络化的趋势，呈现针对特定组织所作的复杂且多方位的 APT 攻击，攻击后留给安全管理人员响应的时间越来越短，使政府用户来不及对入侵做出响应，目的是获取政府内部敏感信息或者对政务网络造成破坏。

三、解决方案

亿赛通可以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。党政军系统内部的数据安全需要从以下几方面解决：

- 1、基于数字证书的统一计算机登录授权管理体系已经成为有效的身份认证基础，在此基础上需要进一步深化数据安全管理；
- 2、需要采用等级保护制度，对文档划分不同的安全等级，对不同等级的文档实现不同强度的安全保护；
- 3、对涉密文档集中式管理，防止分散储存导致的泄密风险；
- 4、对所有笔记本电脑需要全盘加密，有效提高笔记本电脑数据的安全性和保密性，防止被动泄密风险；
- 5、移动存储介质管理，确保移动存储介质的方便性和安全性；
- 6、对所有设备端口必须要进行严格控制，允许合法接入的畅通，同时也要严密防止非法接入；
- 7、针对外发文件，需要加强权限管理，确保外发数据和文件的安全。
- 8、通过病毒恶意攻击是党政军行业重点关注的问题，一旦网络防线被攻破或植入病毒，如果数据本身没有任何加密保护措施，敏感数据泄密的可能性极大。

四、方案价值

- 1、满足党政军行业的合规性要求，为建设强化技术防范、

严格安全管理的信息安全保障体系提供了强有力的技术保证。

- 2、能够针对核心数据资产和非核心数据制定策略，实现数据治理、分级分类管控等精细化的管理。

党政军部分客户案例

- 1、中华人民共和国外交部
- 2、中国航天科工集团
- 3、中国交通部通信信息中心
- 4、北京卫星制造厂
- 5、中国电子科技集团公司第五十三研究所
- 6、中国民用航空华东地区空中交通管理局
- 7、中国工程物理研究院
- 8、中物院六所
- 9、四川航天技术研究院
- 10、广州白云国际机场
- 11、北京市劳动和社会保障局
- 12、泉州市公安局
- 13、宁波市规划局
- 14、保定市国土资源局
- 15、大连船舶重工集团设计研究所有限公司
- 16、湛江港（集团）股份有限公司
- 17、江麓机电集团有限公司
- 18、国家海洋局北海分局
- 19、中国兵器工业第 203 研究所
- 20、陕西省司法厅
- 21、中航工业发展研究中心
- 22、航空工业信息中心
- 23、国网信息通信有限公司
- 24、中核能源科技有限公司
- 25、中国化工经济技术发展中心
- 26、中共中央办公厅秘书局文印中心
- 27、中国兵器集团北方车辆研究所