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

9 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

喜迎 70 华诞，聚焦《亿赛通九月刊》

抢先获悉安全行业最新动态

金风送爽，天高云淡，花果飘香，我们即将迎来祖国 70 周年华诞。在这个丰收与喜悦的日子里，《亿赛通九月刊》与大家共话网络安全大事，共建网络安全环境，共创未来安全。

21 世纪以来，全球科技创新进入空前密集活跃的时期，新一轮科技革命和产业变革正在重构全球创新版图、重塑全球经济结构，这对我国信息化发展提出了新的要求。为贯彻落实新时代中国特色社会主义思想，特别是网络强国战略思想，今年等级保护制度 2.0 相关标准已出台以及国家网信办发布《数据安全管理办法（征求意见稿）》，都表明网络安全已得到国家层面的重点关注。9 月，一年一度的网络安全周再次起航，以“网络安全为人民，网络安全靠人民”为主题在全国开展了一系列网络安全教育活动。目前，网络安全行业在我国还算是小众行业，虽然市场规模不过几百亿，但随着行业得到越来越多的重视，未来市场必定大有可为……

国内

1、《儿童个人信息网络保护规定》将于 10 月 1 日正式实施 净化儿童的网络空间

摘要：儿童是特殊群体，需要给予特殊保护。现实社会里，《未成年人保护法》等法律法规对儿童呵护备至，但谁来为网上世界的儿童保驾护航？日前，国家互联网信息办公室发布了《儿童个人信息网络保护规定》（以下简称《规定》），并将于 10 月 1 日起实施。这是中国第一部专门针对儿童网络保护的立法。

2、APP 超范围采集个人隐私屡禁不绝，怎样避免“裸奔”？

摘要：国家网络安全宣传周，一份来自权威机构对 20 万中国网民的调查报告披露：我国近一半网民认为网络不是那么安全。其中得分比较低的两个指标，一个是近 40% 的网民认为个人信息泄露非常多和比较多，另一个是，近 20% 的网民认为互联网企业履行安全责任情况不太好或非常不好。同样是这一天，网信办、工信部、公安部、市场监管总局点名今日头条、京东金融、云闪付等一批我们常见、常用的手机应用，超范围采集公民的个人隐私。

3、航旅纵横被质疑信息泄露 回应：用户有开启关闭的自主权

摘要：据一名网友反映，在航旅纵横上选座之后，陌生人可以看到自己的名字和头像（并且已经受到骚扰），自己也可以查询到陌生人的名字和头像，质疑航旅纵横泄露客户的隐私。

针对质疑，航旅纵横今天发布微博回应称，该功能是默认关闭的，在本人没有开通虚拟身份前，他人无法看到用户的信息。用户可以随时修改、删除虚拟身份，关闭该功能。用户对该功能有开启关闭的自主权。

4、简历被“明码标价”，谁该为信息泄露买单

摘要：找工作、投简历，在人们看来是再正常不过的一件事，却被“有心人”盯上，用以牟取利益。据《中国青年报》报道，近期，不少求职者在网上投递了简历后，频繁接到陌生电话和短信。网上简历售卖已形成“一条龙”产业，信息被明码标价。

5、嘀嗒出行、自如、斗鱼直播等32 款软件上工信部黑名单

2019 年二季度检测发现问题的应用软件名单

序号	软件/网站名称	域名/网址	所涉问题	应用来源
1	YY	V7.18.1	未经用户同意，收集、使用用户个人信息	网站
2	嘀嗒出行	V8.3.5	未经用户同意，收集、使用用户个人信息	网站
3	斗鱼直播	V5.9.2	未经用户同意，收集、使用用户个人信息	网站
4	返利	V7.6.2	未经用户同意，收集、使用用户个人信息	网站
5	芒果 TV	V6.0.2	未经用户同意，收集、使用用户个人信息	网站
6	美团外卖	V7.13.3	未经用户同意，收集、使用用户个人信息	网站
7	喵播	V4.7.4	未提供账号注销服务	网站
8	自如	www.ziroom.com	未公示用户个人信息收集、使用规则 未提供账号注销服务	网站
9	乐逗游戏	www.idreamsky.com	未提供账号注销服务	网站

摘要：9 月 19 日，工信部官网公布了《2019 年二季度检测发现问题的应用软件名单》。其中，美团外卖、YY、滴答出行、斗鱼直播、返利、芒果 TV、自如等 32 个应用榜上有名。上述名单中，32 个应用所涉及的问题包括“未经用户同意，收集、使用用户个人信息”、“未提供账号注销服务”、“未公示用户个人信息收集、使用规则”、“强行捆绑推广其他应用软件”、“未告知查询、更正信息的渠道”、“恶意‘吸费’”等。

6、抓了 1.8 万人！涉案金额 161 亿！警方铲除百亿“套路贷” 大数据泄露不得不防

摘要：9 月 17 日，广东省公安厅发布消息，粤港澳三地警方 10-11 日开展的一次清查行动期间，广州、深圳、佛山、惠州、东莞等地警方打掉“套路贷”犯罪团伙 16 个，抓获犯罪嫌疑人 140 余人，破获刑事案件 20 余起，查封扣押冻结涉案资产逾 9300 万元。根据公安部 9 月 3 日发布的数据：全国公安机关共侦办“套路贷”团伙案件 1890 起，抓获犯罪嫌疑人 18651 人，破获各类刑事案件 18790 起，查扣涉案资产 161.76 亿元。

7、清洗大数据公司，低隐私权红利是时候终结了

摘要：近期，全国范围内已经有多家大数据公司被查。据自媒体新流财经报道，9 月 6 日下午，多位业内人士称，杭州大数据服务公司——魔蝎数据科技有限公司疑似被相关执法人员控制。与此同时，魔蝎科技为合作方提供的服务已经停止，官网也无法登陆。

8、否认删库跑路剧情，「什么值得买」服务器遭受大面积攻击致罢工数小时

摘要：2019 年 9 月 11 日下午，知名电商导购品牌什么值得买网站及 APP 突然出现故障，持续数小时无法访问的状态。删库跑路的剧本无不充斥着各大论坛、社交平台。而在晚间开始，什么值得买逐步恢复正常的网络访问，并发布致歉公告称“服务器遭受大面积攻击”，目前并未发现数据丢失和泄露。

什么值得买服务异常致歉公告

2019-09-11 22:38:22 0点赞 0收藏 0评论

亲爱的各位值友：

2019年9月11日下午16:00起，因服务器遭受大面积攻击，什么值得买App和网站（www.smzdm.com）出现了服务异常，导致值友无法正常使用。

经过值得买团队的紧急排查、修复，什么值得买App和网站正在逐步恢复正常。目前并未发现数据丢失和泄漏，请各位放心。

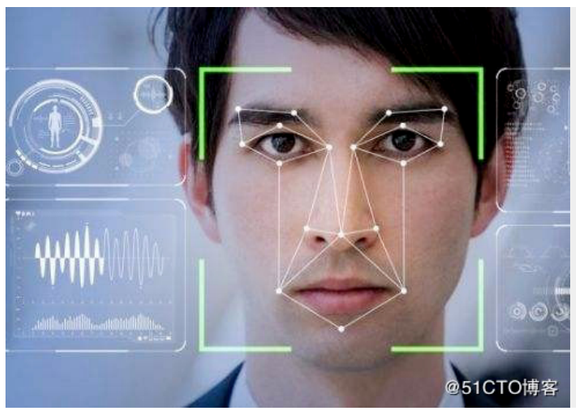
对此给值友造成的不便，我们深表歉意。

对于本次服务器遭受大面积攻击事件，什么值得买公司已经向公安机关报案，公司将积极配合公安机关对攻击源进行追踪。

什么值得买团队已经第一时间联合内部和外部的技术专家成立专项工作组，一起排查问题，避免再次发生类似事件。我们绝不会妥协，也希望与各位值友一起共同抵制黑客行为。

最后再次感谢各位值友的理解和支持。什么值得买将全力为各位值友提供更加优质的优惠信息和内容！

9、法制日报头版刊文谈人脸识别已进校园：数据立法还有多远



摘要：9 月开学季，许多高校在新生报到期间都引进了人脸识别系统，新生到校不再需要复杂的报到流程，只要通过人脸识别系统便可以轻松完成报到。同时，为方便考勤，在上课的教室内，学校也安装了人脸识别系统。但人工智能的功能远不止于此。据了解，通过人脸识别系统，上课期间学生发呆、玩手机等行为都可以被感知。此事引发了舆论的广泛争议，一些网友称此举有侵犯学生隐私和尊严之嫌。

10、近百万条个人信息遭泄露 杭州警方刑拘 8 人

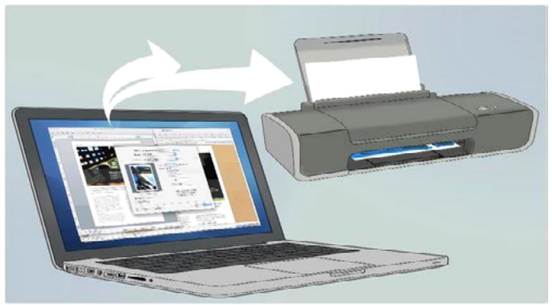
摘要：拱墅警方陆续接到多个电话举报，内容都是一样的，被电话骚扰了。被骚扰的对象都是高管级人物。民警初步侦查发现，频繁骚扰这些人的，是杭州某德健康科技有限公司，而这个公司有一个“不能说的秘密”。这是一家“中介公司”，他们帮上级客户公司电话推广各类健康服务项目。他们每天的工作就是“上网聊天”，然后给“客户”打电话，每个人办公桌上还放着一叠叠“客户”资料。这些“客户”资料的信息很高级，基本都是公司法人代表、管理层人员，姓名、工作单位、联系方式一清二楚，有些甚至连身份证号码都有。

国外

1、数据库泄露了厄瓜多尔大多数公民的数据 其中包括 670 万儿童

摘要：ZDNet 了解到，由于数据库配置错误，厄瓜多尔大部分人口（包括儿童）的个人记录已在网上曝光。这应该是厄瓜多尔历史上最大的数据泄露事件之一，厄瓜多尔是一个拥有 1660 万公民的南美小国。这次泄露的数据库总共包含大约 2080 万个用户记录，这个数据库记录的数量大于该国家的总人口数，其中原因可能来自重复记录或较旧的条目，包含死者的数据。

2、惠普打印机被发现偷偷回传数据：隐藏极深



摘要：据发现，在惠普打印机的安装过程中，有一个很难为人注意的“数据搜集通知与设置”(Data Collection Notice & Settings)，惠普在其中声明会尝试搜集用户的相关打印情况，并传回给惠普，目的是改善广告、用户体验。但是，惠普故意将传回数据类型的选择隐藏了起来，如果不是特别细心、特别懂技术，几乎不可能发现，而且这个“功能”是默认开启的，等于几乎所有用户在使用惠普打印机的时候，都在无意中将自己的相关数据交给了惠普。惠普打印机会搜集所有产生文档的应用的相关数据，基本上你打印的所有类型文档 (txt/doc/jpg/pdf 等等)、时间戳、文档体积、使用报告等等，都在其中。

3、黑客利用“Simjacker”漏洞窃取手机数据 或影响 10 亿人

摘要：网络安全研究人员警告称，SIM 卡存在 “Simjacker”漏洞，该漏洞已经被一家间谍软件供应商利用了至少两年的时间，不过该安全公司并未透露利用这一漏洞公司的名称以及受害者信息。据称，“Simjacker”漏洞攻击包括向手机发送一条短信，短信中包含一种特定类型的类似间谍软件的代码，然后手机会指示手机内的 SIM 卡控制手机，检索并执行敏感命令。这一漏洞存在于称为 S@T 的浏览器中，至少有 30 个国家的移动运营商积极使用 S@T 浏览器技术，总人数超过 10 亿。

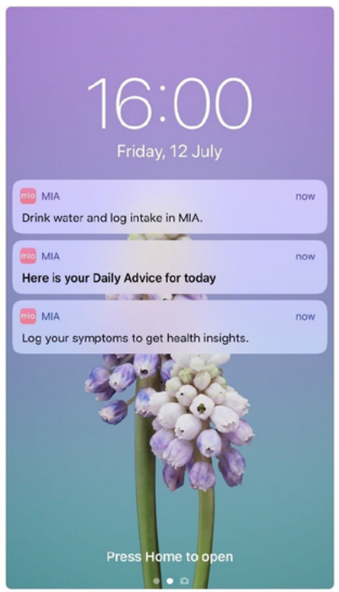
4、贝索斯等 50 多位 CEO 签联名信呼吁国会制定数据隐私法

摘要：包括亚马逊 CEO 杰夫·贝索斯（Jeff Bezos）在内的美国 50 多家大公司的 CEO 日前联名签署一封公开信，呼吁美国国会出台一项全面的消费者数据隐私法案。签署联名信的这 51 位 CEO 来自一系列行业，他们表示，有必要制定一项联邦法律，以确保“对美国消费者进行有力、一致的保护”，并允许“美国公司继续领导一个具有全球竞争力的市场”。

5、四分之一数据泄露背后是人为原因

摘要： 根据 Ponemon 研究机构的最新调查数据，去年所发生的四分之一的数据泄露事件都是人为原因所导致的，而且同期的全部数据泄露事件所带来的平均经济损失约为 392 万美元，跟去年同期相比增长了 1.5 个百分点。而且研究结果还表明，在发生恶意攻击的情况下，事件的修复时间已经逐渐增长到了一年或者更长的时间。

6、拥有上百万名用户的月经追踪应用被指将敏感数据分享给 Facebook

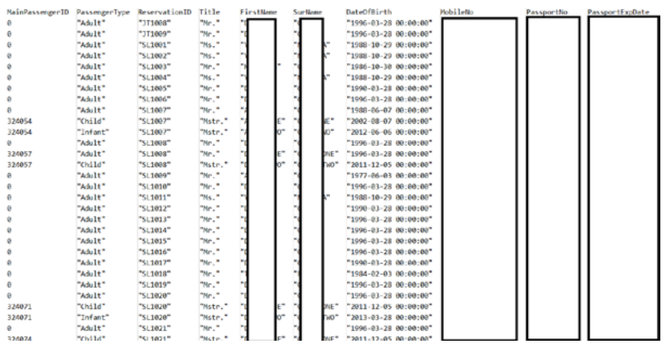


摘要：据外媒报道，一项新的研究发现，经期追踪应用正在向 Facebook 发送有关女性健康和性行为的敏感个人信息。总部位于英国的倡导组织 Privacy International 跟外媒 BuzzFeed News 分享了这一调查结果。该组织发现，包括 MIA Fem、Maya 在内的数款月经跟踪应用会将女性避孕措施的使用情况、月经周期、腹部绞痛等症状等信息直接发送到 Facebook 上。

7、为调查非法武器 美政府令苹果谷歌提交万名用户数据

摘要： 据福布斯杂志网站报道，最近，美国政府希望苹果和谷歌提交使用枪支相关应用的用户数据，包括姓名、电话号码和其他身份识别数据。涉及的用户数量至少有 1 万名。这样的举措前所未有：美国调查人员从未在任何一个案件中，要求苹果和谷歌提价及单个应用的用户个人信息；也从未公开任何一项命令，允许联邦政府要求硅谷巨头一次提交近万人的个人信息。

8、数以百万计的狮子航空旅客记录在论坛上曝光和交换



MainPassengerID	PassengerType	ReservationID	Title	FirstName	SurName	DateOfBirth	MobileNo	PassportNo	PassportExpDate
0	"Adult"	"JT1008"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"JT1009"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"SL1001"	"Ms."	[redacted]	[redacted]	"1988-10-29 00:00:00"			
0	"Adult"	"SL1002"	"Ms."	[redacted]	[redacted]	"1988-10-29 00:00:00"			
0	"Adult"	"SL1003"	"Mr."	[redacted]	[redacted]	"1986-10-30 00:00:00"			
0	"Adult"	"SL1004"	"Ms."	[redacted]	[redacted]	"1988-10-29 00:00:00"			
0	"Adult"	"SL1005"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"SL1006"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"SL1007"	"Mr."	[redacted]	[redacted]	"1988-06-07 00:00:00"			
324054	"Child"	"SL1007"	"Mstr."	[redacted]E"	[redacted]E"	"2002-08-07 00:00:00"			
324054	"Infant"	"SL1007"	"Mstr."	[redacted]O"	[redacted]O"	"2012-06-06 00:00:00"			
0	"Adult"	"SL1008"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
324057	"Adult"	"SL1008"	"Mr."	[redacted]E"	[redacted]NE"	"1996-03-28 00:00:00"			
324057	"Child"	"SL1008"	"Mstr."	[redacted]O"	[redacted]NO"	"2011-12-05 00:00:00"			
0	"Adult"	"SL1009"	"Mr."	[redacted]	[redacted]	"1977-06-03 00:00:00"			
0	"Adult"	"SL1010"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"SL1011"	"Ms."	[redacted]	[redacted]	"1988-10-29 00:00:00"			
0	"Adult"	"SL1012"	"Mr."	[redacted]	[redacted]	"1990-03-28 00:00:00"			
0	"Adult"	"SL1013"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"SL1014"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"SL1015"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"SL1016"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"SL1017"	"Mr."	[redacted]	[redacted]	"1990-03-28 00:00:00"			
0	"Adult"	"SL1018"	"Mr."	[redacted]	[redacted]	"1984-02-03 00:00:00"			
0	"Adult"	"SL1019"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
0	"Adult"	"SL1020"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
324071	"Child"	"SL1020"	"Mstr."	[redacted]E"	[redacted]NE"	"2011-12-05 00:00:00"			
324071	"Infant"	"SL1020"	"Mstr."	[redacted]O"	[redacted]NO"	"2013-03-28 00:00:00"			
0	"Adult"	"SL1021"	"Mr."	[redacted]	[redacted]	"1996-03-28 00:00:00"			
324074	"Child"	"SL1021"	"Mstr."	[redacted]E"	[redacted]NE"	"2011-12-05 00:00:00"			

摘要：LionAir 旗下两家航空公司的客户提供的数千万份记录已经在数据交换论坛上流传了至少一个月。这些记录存在于两个数据库中，一个数据库有 2100 万个记录，另一个数据库有 1400 万个条目，目录中保存着 2019 年 5 月创建的备份文件，主要是为 Malindo Air 和泰狮航空创建的。另一个备份文件的名称是 BatikAir，该航空公司的母公司也是 LionAir。泄露的详细信息包括乘客和预订 ID、物理地址、电话号码、电子邮件地址、姓名、出生日期、电话号码、护照号码和护照有效期。

9、美国养老金系统发生网络盗窃事故，损失达 420 万美元

摘要：近日，黑客设法从俄克拉荷马州执法人员的养老金系统中窃取了大约 420 万美元的资金。联邦调查局在接到报告后展开了调查。据了解，该养老金系统一名雇员的电子邮件帐户曾被黑客盗取，随后便发生了养老金盗窃事件。这笔资金由养老金系统委托一名外部投资经理进行管理。负责人称，该机构能够找回大约 477000 美元的被盗资金。专家表示，美国国家养老金和薪资系统已经成为热门攻击目标，因为此类系统通常拥有大量资金，但有时却会使用过时的安全技术。2016 年，黑客从美国宾夕法尼亚州的一个警察养老基金中窃取了 10 万美元。2017 年，黑客窃取了爱荷华州超过 100 名公务员退休人员的养老金。

10、曝全球最大加密货币交易所发生数据泄露事故

摘要：近日获悉，全球最大的加密币交易所 Binance 发生了信息泄露事件，导致数百名用户的身份证明图像被发布到网上，未来还可能影响上万用户。待进一步了解得知，此次泄露的身份证明图像被称为“客户了解”（Know Your Customer，即 KYC）图像。目前，Binance 方面已经证实，黑客公布的 KYC 图像中，有一部分与事实相符，但其他图像或是虚假图像，且种种迹象表明，被泄露的图像可能已被用于更改账户信息和设置成诈骗账户。

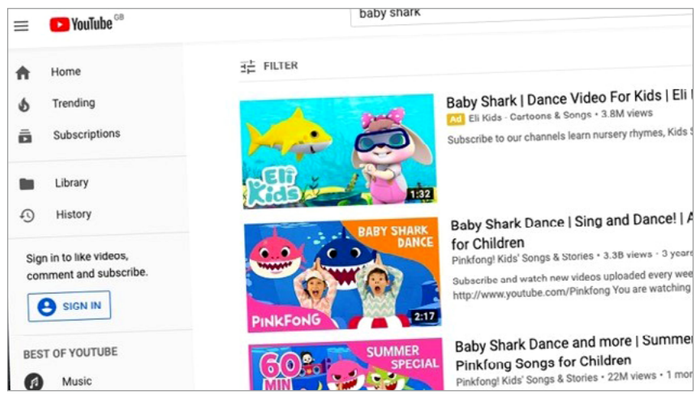
11、调查显示，英国超 8 成学校曾遭受网络攻击

摘要：据外媒报道，近日，英国国家网络安全中心（National Cyber Security Centre）与网络服务供应商 London Grid for Learning 展开合作，对英国的 430 多所学校进行了网络安全审计。审计发现，几乎所有学校（97%）都表示，无法访问学校系统会造成严重后果，但绝大多数学校（83%）都曾遭受过网络攻击。数据显示，69%的学校曾遭受过网络钓鱼攻击，30%的学校曾感染过某类恶意软件，20%的学校的内部邮箱曾被用于诈骗，还有 35% 的学校曾因遭受网络攻击而无法访问重要文件。

12、韩国工业供应商 DK-Lok 数据库被曝不设防

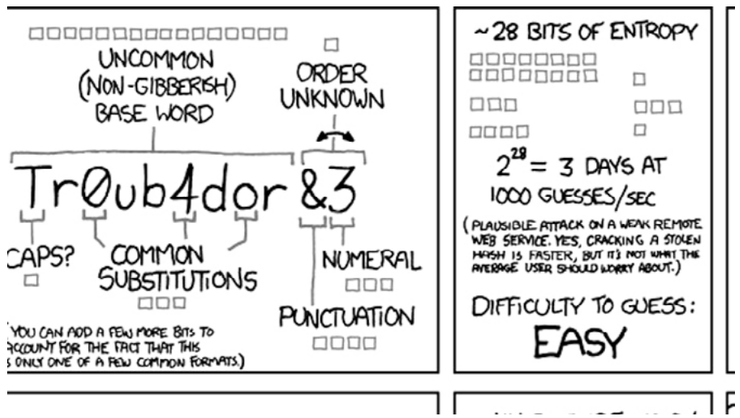
摘要：近日，网络安全公司 vpnMentor 发现，韩国工业供应商 DK-Lok 的一个数据库并未设置任何身份验证措施，导致该数据库内部信息可被公开访问。

13、谷歌 YouTube 因非法收集儿童个人信息被罚 1.7 亿美元



摘要：美国联邦贸易委员会（FTC）称，Alphabet 旗下谷歌公司及其 YouTube 视频服务将支付 1.7 亿美元和解金，以了结有关 YouTube 收集儿童个人信息并因此触犯了联邦法律的指控。YouTube 被控在未经父母同意的情况下使用“cookies”追踪儿童频道的观众，并借此向这些观众投放了价值数百万美元的靶向广告。

14、人气网络漫画 XKCD 论坛遭网络攻击：大量用户数据被盗



摘要：据外媒报道，黑客攻击了人气网络漫画网站 XKCD 的论坛并从中窃取了约 56 万个用户名、电子邮件和 IP 地址以及散列密码。XKCD 在周末公开了这次攻击，此前，负责数据漏洞通知网站 Have I Been Pwned 维护工作的安全研究员 Troy Hunt 向该网站发出了警告。现在，这个论坛已经下线。

精彩不停，掌声不断！ 2019 年网络安全周活动亿赛通实力护航信息安全

金桂飘香时节，全国奏起网络安全协奏曲。9 月 16 日，2019 年国家网络安全宣传周活动正式启动。

亿赛通本届大会共参展山东省及辽宁省双项活动，为社会大众普及网络安全知识，带来了数据安全信息管控、安全态势感知等解决方案，重点展示亿赛通在企业网络安全、数据安全及公民个人隐私保护等方面的技术研究成果，以实力护航国家、企业及个人信息安全。

党的十八大以来，党中央高度重视网络安全建设。没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。国家更是对加快推进新时代网络强国建设作出了全面部署，《国家安全法》《网络安全法》等法律法规相继制定出台，在新形势下促进网络安全产业新发展。

实力护航信息安全

作为数据安全领域的一线知名厂商，亿赛通本次展会通过全方位综合解决方案，立体展示公司在协助政府部门、知名企业进行网络安全数据安全信息监管、数据泄露防护、个人隐私保护等方面取得的成就。在展出一系列相关的安全产品以外，亿赛通还向观众分享各种网络攻击行为给我们日常生活所带来的安全威胁，让观众更直观的理解生活中的网络安全隐患，帮助观众提升网络安全意识。

网络安全周辽宁站

网络安全周山东站

除了于特定环境建立防护网，主动打击、遏制网络信息传播，网民安全意识的培养与提升也是构建网络安全的重要手段之一。我司将积累的真实案件与沉淀的丰富数据开创为多种形式的宣传素材，持续对外界输出网络安全知识，并结合海量数据泄露状况深入分析与调研，为治理网络诈骗提供技术支撑，使得网络安全意识教育更有针对性和前瞻性。

亿赛通希望通过此次网络安全博览会参展，提升大众在网络安全方面的意识，并且呼吁大众积极参与到网络安全建设的阵营当中，保护好国家、企业、个人数据信息安全，同时也为净化网络安全环境贡献力量，携手国家合力共建“网络强国”！

媒体专访——扬技术研发优势 促数据安全领域深耕

文章来源于中国信息安全记者

近些年，随着信息技术的不断发展，云计算、物联网、大数据等新兴技术在当今社会里扮演着越来越重要的角色，政府、企业和个人在享受新技术带来的巨大便利的同时，也必然要承担其产生的风险。其中，数据安全问题是近几年网络飞速发展所凸显的严重问题之一，勒索病毒爆发、重要数据及个人信息泄露事件的频频发生，一方面体现了数据在当今社会的重要价值，另一面也为我们拉响警种，做好数据安全防护已迫在眉睫。

从 2017 年《网络安全法》的实施，到今年等级保护制度 2.0 相关标准的出台以及国家网信办发布《数据安全管理办法（征求意见稿）》，都表明数据安全已得到国家层面的重点关注。在《中国信息安全》杂志举办的“2018 年度网络安全十大热词”评选活动中，数据安全和信息泄露更是成为网民关注度最高的两个词汇。可见，在这个“数据为王”的网络时代，政府、企业和个人都开始高度重视数据安全问题，做好数据安全防护必将是未来信息安全工作的重中之重。

扬技术专长，深耕行业市场

随着互联网的飞速发展，国家政府的运转、企业的业务开展以及个人的日常生活都与网络联系的愈加紧密。数据是网络时代信息传递和储存的根本，其价值不言而喻。数据早已成为网络攻击者和不法分子的头号目标。做好数据安全防护，不仅需要国家政府出台相应的法律法规进行监管，同时也离不开网络安全企业提供专业的技术服务。

以做“中国数据安全防护专家”为企业口号的亿赛通，是一家深耕数据安全领域多年的网络安全公司。在赛迪顾问发布的《中国数据泄露防护产品市场研究报告（2019）》中，亿赛通再次以 17.7% 的市场占有率排名第一，更是连续四年拿下榜首位置。在亿赛通副总经理李贺看来，这与公司多年来专注技术研发积累、深耕行业市场是分不开的。

李贺谈到，网络安全近年来得到了越来越高的重视，企业和个人数据受到攻击和泄露等严重事件的频频发生，让大家不仅意识到数据资产的价值，更是把数据安全防护意识提到了一个新的高度。早些年，企业数据的泄露可能只会关系到知识产权的相关问题，现在，数据安全问题则会关系到相应的法律责任，甚至是企业的生死存亡。

他认为，网络安全行业是一个技术性非常强的行业，是需要多年的基础研发和技术积累才能做好的一个行业。自 2014 年被绿盟收购以来，亿赛通始终发挥自身技术优势，这点与同样以技术见长的绿盟不谋而合，这对亿赛通的业务发展更是起到了促进作用，为近几年所提交的满意市场答卷奠定了基础。亿赛通十多年来始终坚持自主研发，在近几年的产品研发及投入上不断加大筹码，很多安全产品、安全理念和安全服务都在行业内处于领先地位。

做好基础研发，升级产品服务

目前，网络安全行业在我国还算是小众行业，市场规模也不过几百亿，但李贺认为，随着数据安全得到越来越多的重视，未来市场必定大有可为。如何能在发展快速、竞争激烈的市场中保有一席之地？他表示，专注于细分行业，保持技术优势，发挥产品特色，持续不断地深耕行业市场，持续不断地进行自主技术研发，是维持企业自身长期竞争优势的根本所在。

2018 年，亿赛通正式成立武汉第二研发中心，开启北京、武汉双核研发驱动模式。李贺表示，武汉研发中心的建立进一步增强了公司的技术研发能力，拓展了公司人才培养的渠道，为公司未来业务更好的发展奠定了基础。同时，研发中心选址武汉东湖高新区（位于中国光谷核心地段），与各大科技公司毗邻，利于公司融入外部创新、开放、包容的文化环境，为企业注入创新活力和发展动力提供了便利条件。

北京亿赛通科技发展有限责任公司副总经理
李贺

李贺认为，在国家政策支持下，数据安全市场将会越来越具优势，随着国家对国产化安全要求的提高，未来数据安全的市场份额占网络安全市场的比例会逐步上升。在这样的情况下，亿赛通更是要做好以下四点：沉淀经验和服务，蓄势待发；打造综合型服务，多行业多领域布局；携手渠道伙伴，构建完善服务体系；加大研发投入，持续创新。向成为世界级的数据安全企业不断迈进。

数据正在成为人类社会极为重要、不可或缺的一部分，它或好或坏地影响着社会的方方面面。善用数据，保护好数据将会是未来全世界需要长期重点研究的课题。亿赛通将继续其企业使命，为客户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。

高中生的“数据帝国”梦，天才黑客竟是未成年

自学软件编程技术，研发黑客软件，利用网站注册漏洞疯狂盗取公民个人信息上亿条，在境内外网络上公开售卖……

刚满 18 岁的高中生，竟构想出一个非法“数据帝国”梦。

黑客遭举报牵出侵犯公民个人信息大案

2018 年 9 月，警方接到网友举报，有人在论坛、贴吧等平台售卖公民个人信息以及盗窃信息所用的黑客软件，警方第一时间跨省抓捕了 26 岁的江西籍犯罪嫌疑人付某。

付某交代，自己对软件编程和黑客技术有着浓厚的兴趣，于 2018 年初在某网络交流论坛中向一个网友请教获取他人个人信息的方法，并从对方处购买了一款黑客软件用于获取公民个人信息。

自 2018 年 5 月至 8 月，付某利用购得的黑客软件攻击各网站系统漏洞，非法获取公民个人信息，将该黑客软件升级后，通过网络论坛等渠道以每月 500 元的价格大肆售卖，累计侵犯公民个人信息 200 多万条，非法获利上千元。最终，法院以侵犯公民个人信息罪判处付某有期徒刑三年零六个月，并处罚金 3000 元。

付某在审讯过程中交代了出售给他黑客软件的网友叫“i 春秋”，警方顺藤摸瓜挖出一个更大的网络侵犯公民个人信息案。

只因对盗取公民信息有兴趣自学网络技术

通过对“i 春秋”这一网名在网络全域展开技术调查，警方确定“i 春秋”网名使用者为刘某。同时，警方发现刘某涉嫌盗取公民个人信息，在境内外网络公开售卖。

经过调查后，刘某竟是信宜某高级中学的高三在校生，刚满 18 周岁。刘某被警方带走后，该校教师和同学始终不敢相信，这样一个普普通通即将奔赴高考的高中生会是一个精通网络技术，盗窃公民个人信息的黑客。

经查，刘某从小就对计算机十分感兴趣，经常利用节假日操作电脑，自学计算机技术，还通过翻墙软件浏览境外网站“取经”，到高中阶段，刘某已掌握独立编写软件程序的能力。

据刘某交代，从 2017 年下半年开始，其在各大论坛、贴吧看到查询网络用户个人信息的方法，对此产生了兴趣，就想能通过自己学到的技术获取他人的个人信息。

不出一个月，刘某编写出一款软件，通过内置接口，，将其对接到各网站后，便可轻松获取到网站用户账号和对应的手机号码，后将该程序卖给付某等人。但很快刘某发现该软件操作繁琐，且不能批量获取信息。2018 年 7 月，刘某在网络论坛中找到了解决方案，开始计划构建属于自己的“信息数据库”。

为不让同行发现主动向网站反馈漏洞

受到启发后，刘某又编写出了一款能够批量获取信息的软件，将软件接口与某网站对接，轻松获取了该网站的用户账号以及对应手机号码。为了建立自己的“数据帝国”，刘某租用了网络数据对信息进行储存，并专门在境外租用十多台服务器支持操作。

一个月的时间，刘某非法获取了约 1 亿条公民个人信息，全部存储于自己的数据库中。

为了不让其他同行发现漏洞，刘某曾向自己盗取过个人信息的网站反馈，将网站存在的漏洞进行封堵。此后，刘某在境内网络建立起微信、QQ 群，在境外使用“telegram”等聊天工具，自助编写“信息查询”机器人，将数据库通过微信、QQ 等群聊以包月查询的形式向他人兜售，并且在境外以比特币为交易货币贩卖数据库长达两个月，共计获利近 2 万元。

按照刘某的设想，他将会对数据库中上亿条个人信息进行整理，进而获取用户名、手机号码对应的真实姓名、家庭地址等公民个人信息，利用技术手段实现经纬度实时定位，从而建立起一个强大的“数据帝国”。

承办检察官指出，该案数据总量大，非法获取公民个人信息精准，危害公民个人信息安全甚至是国家数据信息安全，应当对犯罪嫌疑人刘某批准逮捕。承办检察官在办案中发现刘某由于长期沉浸于网络“虚拟世界”，价值观和心理健康受到影响，正在聘请专业的心理咨询师对刘某进行心理疏导，逐步引导其走上正确道路，积极面对未来人生。

计算机、互联网的发展虽然让我们的生活得到便利，让学生能足不出户了解更多知识，但过度的信息来源也给学生带来不一样的诱惑，同时也越来越让我们的信息暴露在公众之下。针对现在各种黑客入侵泄密，除了安全防护技术需要不断加强，法律、制度也应更加完善，信息安全、数据安全的立法也要加快进程。同时，未成年人在学习互联网技术的时候，应当认识到信息泄露的严重性，有保护信息安全的意识。不过，在我国未来法律越来越健全的形势下，不法分子“捡漏”的机会将越来越低。亿赛通也将继续专注数据安全领域，为国家、企业、个人的信息安全保驾护航！

文章资讯来源于互联网

官方清洗数据黑产，大数据行业如履薄冰

前所未有的“清洗”

国内的第三方数据公司们正在遭遇一轮前所未有的“清洗”。从上周开始，全国范围内已经有多家大数据公司被查。媒体报道，某第三方数据服务公司发出通告称，停止了对外提供用户授权的运营商爬虫服务。此外，还陆续有消息传出，其他大型的第三方数据服务公司或停止服务、或高管被警方带走。

“整个行业都快抓没了。”多位数据行业从业者表示，他们已经基本停工观望。据知情人士透露，几十家大数据公司已进入调查名单，“这只是前戏”。数据行业，可能面临诞生以来最艰难的时刻……

灰色合作导致业务被波及

据相关人士爆料，此次被约谈的企业领导均曾与爬虫公司合作，其中不乏国企，被调查公司的合作公司都可能被牵连。某爬虫公司被调查之后，与之合作的一家金融科技机构也被警方要求协助调查。尽管第二天，金融公司的人被放了出来，但业务仍旧受到了影响。现在，整个大数据行业，包括与数据行业合作较多的行业，都噤若寒蝉，如履薄冰。

严查数据贩卖黑产

这两年，大数据行业的发展极为迅速。数据黑产的增长，尤其激进：爬取通讯录，借贷用户数据被随意贩卖，以进行电话、短信营销等等。

某公司创始人称：大数据行业有黑色的操作，有灰色的操作，但行业唯一没有找到的，是“光明正大的合规操作”。刚开始，大家以为只抓“爬虫公司”，行业排名靠前的爬虫公司都陆续被调查。

大数据公司业务全部暂停

多家大数据公司 CEO 一致宣布：业务全部暂停。并且，曾经合作过的公司，为免受到数据滥用、泄露、贩卖等问题的波及，要求他们签署“免责条款”或者“承诺书”。

（1）我公司在以往经营活动中，无违法违规记录，没有因数据归属、采集、使用等问题发生过法律纠纷或接受过行政处罚。

（2）我公司近三年业务往来中，不存在法律纠纷，无不良记录。

（3）在服务合作期内，我公司提供的数据服务，符合国家法律法规和行业监管部门的有关规定，且数据来源合法合规。

（4）我公司提供的服务结果均为实时数据的查询结果，不存在使用以往留存的陈旧信息问题，且我公司不留存贵公司的个人信息数据及获得的查询结果。

官方出手严查数据黑产

2019 年，大数据行业密集发生的丑闻不断出现在公众视野：先是“315”晚会集中曝光的大数据黑色产业链，后有号称拥有全国最大数据库的招聘类数据公司巧达科技被爆利用爬虫手段获取简历中的用户信息并变现。

与此同时，一系列关于互联网隐私保护、个人信息安全的监管办法也相继推出。国家互联网信息办公室公布了《数据安全管理办法 (征求意见稿)》以及《网络安全审查办法 (征求意见稿)》、《儿童个人信息网络保护规定 (征求意见稿)》等。

不难发现，与其他领域的监管整治不同，对于数据公司违法行为的打击力度从一开始就是最为严厉的，由公安部门直接介入，但即便如此也很难彻底肃清。

目前，整个行业都在停业观望，并感受着行业诞生以来的最大动荡。但毋庸置疑的是，这是刮骨疗伤必然经历的巨痛，解决大数据行业通病刻不容缓。

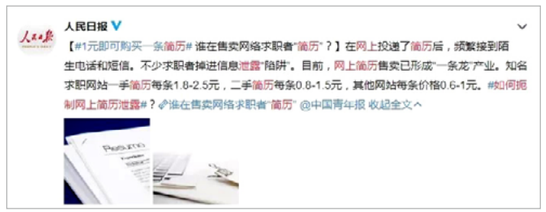
而对于数据安全行业来说，人为的恶性攻击相对自然灾害而言显得更为复杂多变。“什么是敏感数据？敏感数据在哪？需要控什么？需要怎么控？”等问题已成为大家高度关注的焦点，在数据的全生命周期过程中，任何一个环节都不容忽视。针对企业外部恶意攻击、内鬼泄露等问题，以产品作为辅助工具加强企业安全防御，通过服务 + 产品形成一体化服务更为稳妥。 亿赛通始终用实力、事实说话，为用户打造一个界限明确、放心可靠的数据安全环境。

文章资讯来源于互联网

简历贩卖价格创新低，一元贱卖中

微博热搜榜高高挂起的话题，个人简历泄露事件被推上风口，一张 A4 纸上填满的都是我们最隐私的个人信息，却无法被 100% 保护……

大数据时代，所有信息都被录入，每个人就像是皇帝的新衣，全民“裸奔”！但正因为“全盘托出”，安全也出了“故障”，个人隐私泄露也已经不是第一次发生了，总有无良商家做着这类见不得光的“黑生意”，以 1 元，甚至是几毛的价格批发兜售个人信息，而这种事情就如漏网之鱼一样，抓不完只能望着黑心商户早日醒悟，这是违法。



网友们纷纷吐槽，隐私被泄露真的不要太可恶，被骚扰、被通知、被诈骗，都呼应赶紧将网络安全规范化，让这些不法分子都尽快绳之以法，也有像小亿一样习以为常的反嘲，毕竟也是接过来自美国、德国电话的人呢 ~

网上简历售卖已经形成“一条龙”产业，既然避免不了被泄露，那就自己注意点吧！如今市场上五花八门的 App 越来越多，谁说手机上没个 20 款 App 小亿都不信且几乎每款都需要注册个人信息，至于是否像 App 隐私保护政策说的那样安全可靠，咱也不清楚。

但拥有最多个人信息的平台一定是招聘类的网站了，每个人求职路上少说也通过 3 个招聘平台发布过个人简历，这严重的个人信息泄露事件，让人不禁联想，咱的身份信息，说不准已经在这神州大地都去遍了。

今年也有多次相关招聘网站被曝出：内部员工低价贩卖 16 万份简历，每份简历以 5 元的成交价格售出。这 .... 这么大的金额数目 , 那可是要↓↓↓

总而言之 , 小亿希望我们把隐私交到各平台时，都能够得到平台承诺的安全保密，更希望未来的网络安全更加坚固，让这些漏网之鱼无洞可钻！

亿赛通成功签约中国建设银行

客户简介

中国建设银行成立于 1954 年，是股份制商业银行，国有五大商业银行之一。中国建设银行主要经营领域包括公司银行业务、个人银行业务和资金业务，中国内地设有分支机构 14121 家（2012 年），在香港、台湾、墨尔本等地设有分行，拥有建信基金、建信租赁、建信信托、建信人寿、中德住房储蓄银行、建行亚洲、建行伦敦、建行俄罗斯、建行迪拜、建银国际等多家子公司，为客户提供全面的金融服务。中国建设银行拥有广泛的客户基础，与多个大型企业集团及中国经济战略性行业的主导企业保持银行业务联系，营销网络覆盖全国的主要地区。

典型案例 TYPICAL CASES

需求背景

中国建设银行作为中国大型国有银行，其业务体系非常庞大复杂，面对互联网以及信息化大爆炸时代，企业数据面临着极大的风险，为防止建行内部敏感数据泄露出去，建行携手亿赛通部署了文档安全产品，保障其数据无懈可击。

解决方案

亿赛通文档安全管理系统防止建行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。

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

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。

离线办公支持：系统提供安全离线办公业务支持，通过离线审核、策略预设及离线补时等功能满足各类离线办公要求。

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。

细粒权限控制：不仅可细化设置文档的阅读、编辑、复制、打印等组合权限，还可根据管理需要设定文档生命周期，同时提供灵活的二次授权管理、归档管理、交接管理及版本变更管理等功能。

安全浮水印支持：为保障核心数据的打印安全以及可追溯性，系统提供对加密文档的阅读和打印浮水印功能，通过自动添加安全警示及版权标识信息来降低屏幕录制和自主打印带来的泄密风险。水印支持自定义。

项目成果

亿赛通文档安全产品加强了建设银行的内部网络系统安全、有序、高效的进展，提高其数据安全的智能化管理。

亿赛通成功签约上海浦东发展银行股份有限公司

客户简介

上海浦东发展银行股份有限公司成立于 1992 年，经中国人民银行批准设立、1993 年 1 月 9 日开业，1999 年在上海证券交易所挂牌上市（股票交易代码：600000）的全国性股份制商业银行，总行设在上海。目前，注册资本金 196.53 亿元，优秀的业绩、良好的声誉，使浦发银行成为中国证券市场中备受关注和尊敬的上市公司。 自公司上市以来，浦发银行连续多年被《亚洲周刊》评为“中国上市公司 100 强”，并且公司一直秉承“笃守诚信，创造卓越”的核心价值观，积极探索金融创新，资产规模持续扩大，经营实力不断增强。

需求背景

随着浦发银行各项业务的迅猛拓展，信息技术是其业务实现的重要平台，那么信息作为浦发银行的重要资产，是其赖以生存、发展的基础。虽浦发银行对预防信息泄露措施做得比较周全，但是随着大数据、互联网、云计算、人工智能等新的革新方式不断发展壮大，信息安全将会面临更大威胁。所以浦发银行对信息安全可能产生的问题及存在的风险漏洞仍需继续加强预防，即采取措施来保护和控制银行内部数据、信息不被非法访问、读取，病毒入侵，黑客攻击。

解决方案

亿赛通可信介质（简称 MediSec）安全管理系统是针对移动存储介质使用范围、使用方式及数据安全存储进行科学控制的安全管理系统。

MediSec 通过对介质的访问控制与注册授权，实现非注册介质接入内网计算机上不能使用，以及内网专用介质接入非内网计算机上不能使用。数据始终以密文形式存储在专用介质上，非授权用户不能解密，保证涉密介质丢失后不会造成泄密事故，同时用户用 U 盘拷贝数据时可以实时备份到服务器上，便于日后追溯审计。详细的介质使用审计日志，确保介质可追踪。这里的介质涵盖：U 盘、移动硬盘、手机、数码相机、摄像机、ipod、MP3/MP4、PDA、各 CF/MD/SD/Flash Disk 等移动存储设备。

项目成果

浦发银行通过部署亿赛通可信介质安全管理系统后，达到了如下效果：

进不来：非注册介质不能在单位内部计算机上使用。

拿不走：内部注册专用 U 盘不能在单位外界计算机上使用。

读不懂：内部专用 U 盘数据进行加密存储，非授权用户不能解密。

改不了：数据存储在专用 U 盘上，非法用户无法更改数据内容。

走不脱：详细的 U 盘使用日志，泄密事件可追踪，犯罪分子无处可逃。