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：86-10-57933600

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

6 月刊

2018 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 座三 / 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

安全圈最新大事件

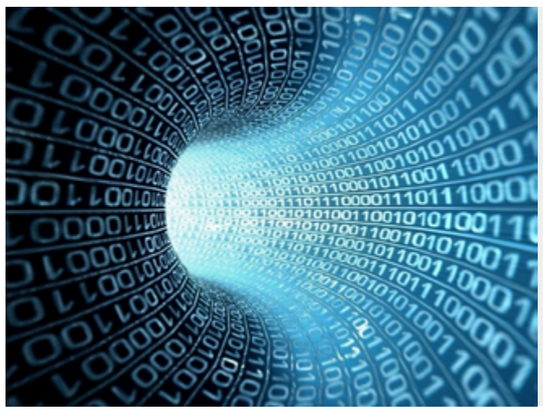
随着大数据、人工智能的快速发展，使各行各业对电子化的依赖不断加强，数据文件成为企业的重要资产之一，是现代商业的命脉，关乎企业的生存与发展，数据安全市场需求愈加强烈。由此，建立并完善企业数据安全体系至关重要，它有助于我们从企业的发展战略高度，清醒的认识数据安全所带来的诸多冲击。亿赛通现有的产品及解决方案涵盖了系统监控与审计、电子文档加密、敏感数据防护、网络入侵防御、移动存储介质防护等多个方面。并在六月全新推出“勒索病毒防护卫士”，从源头上真正的保护用户数据安全，打击非法勒索黑产，中国数据安全防护专家——亿赛通，有着义不容辞的责任。

国内

1、12306 信息泄露”是虚惊也是警示

摘要：据中国铁路总公司官方微博消息：6 月 13 日，网传“12306 数据疑似泄漏”。经核查，该网站未发生用户信息泄漏，网传信息与铁路 12306 网站无关。

2、如何防止大数据时代个人隐私的“裸奔”



摘要：21 世纪是数据信息飞速发展的时代，移动互联网、物联网、社交网络、电子商务等极大拓展了互联网的边界和应用范围，各种数据正在快速膨胀变大，整个社会已经步入大数据时代。但大数据是把双刃剑，国家和企业因大力推动大数据创新应用而获益的同时，也给个人信息安全尤其是隐私信息的安全带来巨大威胁。

3、交易 1800 余条公民房屋产权信息，上海一征信公司被公诉

摘要：5 月 17 日，该案由虹口区人民检察院对该公司及员工向法院提起公诉。6 月 12 日下午，虹口区人民检察院召开新闻发布会，对该案及此类案件的办理情况做了通报。

4、A 站近千万条用户数据外泄！含账户密码，称受黑客攻击已报警

摘 要：6 月 13 日 凌 晨，AcFun 弹幕视频网（俗称：A 站）在其官网发布《关于 AcFun 受黑客攻击致用户数据外泄的公告》称，AcFun 受黑客攻击，近千万条用户数据外泄，包含用户 ID、用户昵称、加密存储的密码等信息。

5、江苏披露一起案件侦破经过，警方出重拳守护个人信息安全


选聘社会监督员 正风肃纪进村屯

11 政治

智方出重拳 守护个人信息安全

党员模范汇 宣讲进社区

学习与研究

中共党史研究

摘要：日前，江苏警方披露了一起侵犯公民个人信息案件，常州市公安局网安支队挖出一条个人信息黑市交易链，共抓获 48 名行业部门内鬼和 82 名中介商。这是去年“两高”司法解释出台后，公安部挂牌督办的第一起侵犯公民个人信息案。

6、《贵阳市大数据安全管理条例》将实施：明确数据安全第一责任人

摘要：新华社贵阳 6 月 5 日电（记者刘智强）5 日，《贵阳市大数据安全管理条例》（以下简称《条例》）经贵阳市第十四届人大常委会第十三次会议表决通过。

7、航旅纵横 App 在泄露隐私边缘试探

摘要：航旅类 App 航旅纵横因最近上线的“虚拟客舱”功能引发争议。通过这个功能，用户可以查看同舱乘客的历史飞行地点及频率等信息，还可以与同客舱的乘客进行私聊。有网友担心，该功能存在隐私泄露隐患。

8、蔡徐坤未播音频被泄露 NINE PERCENT 发声明粉丝要求维权！

摘要：近日，NINE PERCENT 的队长蔡徐坤未播音频曝光，在音频引起热议后，粉丝强烈要求维权！表示只想追究私录视频及泄露音源的所谓工作人员。希望爱豆世纪能够保护好艺人的合法权益，保护好艺人的个人信息！

9、警惕！随手点赞易泄露个人信息

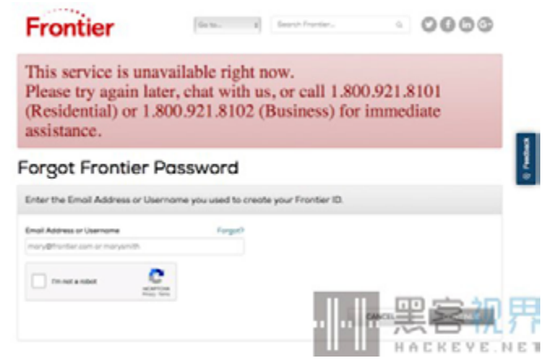
摘要：如今，社交媒体深入了大多数网络用户的生活，尤其是许多年轻人，很爱在社交媒体上分享自己的日常生活，随手点赞、转发也成了很多社交媒体用户的习惯。可是你知道吗？一次简单的点赞就可能让你的个人信息在不知不觉中泄露出去了。

10、“呼死你”电话响不停 信息泄露惨遭“精准骚扰”怎么办？

摘要： 近日，警方在四川、河南、广东等多个省市同步开展打击“呼死你”黑灰产业链专案收网行动，成功打掉“疯狂云呼”和“呕死他”等两个“呼死你”犯罪团伙，以及线下利用“呼死你”平台进行非法追债的 3 个犯罪团伙。

国外

1、美电信巨头 Frontier 曝密码重置漏洞 只需用户名就能登陆任意账户

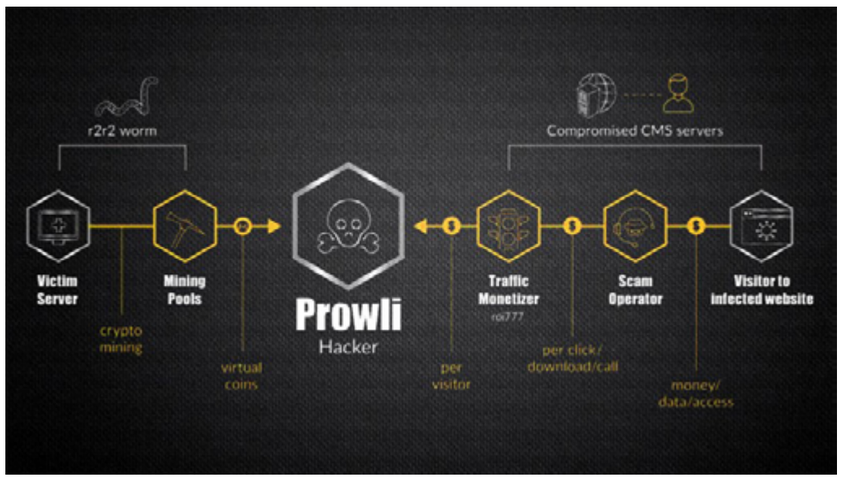


摘要：Frontier Communications（以下简称“Frontier”）是美国的一家语音、视频和互联网服务提供商，也是美国最大的互联网提供商之一。根据外媒 ZDNet 的报道，安全研究员 Ryan Stevenson 发现密码重置漏洞允许攻击者绕过密码重置过程中发送的访问代码。

2、数据泄露影响超过 1000 万公民 马来西亚教育部 SAPS 系统紧急下线

摘要：据马来西亚媒体 Malay Mail 报道，在发现存在一个可能暴露超过 1000 万公民个人信息的安全漏洞之后，由马来西亚教育部推出的学校考试分析系统（Sitem Analisis Peperiksaan Sekolah，SAPS）被迫紧急下线。

3、黑客积极利用 Prowli 僵尸网络获利 全球已有超过 4 万台设备沦陷



摘要：GuardiCore 安全团队在本周三（6 月 6 日）发布的一份报告中指出，他们发现了一起大规模的流量操纵和加密货币挖掘活动，影响了金融、教育和政府等行业的众多组织。

4、HR 软件公司 PageUp 遭恶意软件感染 超过 200 万用户个人信息或已泄露

摘要：据外媒 ZDNet 报道，总部位于澳大利亚的人力资源（Human Resource，HR）软件公司 PageUp 已经证实，它的 IT 基础设施在上个月被发现存在异常活动，这可能会导致客户数据的泄露。

5、特斯拉起诉前员工盗取并泄露公司内部数据

摘要：本周三，据美国内华达州联邦法庭公布的诉讼文件显示，特斯拉起诉了一名前员工，称其盗取了该公司的商业机密并向第三方泄露了大量公司内部数据。

6、 DNA 检测公司 MyHeritage 遭黑客入侵：9200 万账户泄露

摘要：北京时间 6 月 6 日早间消息，消费级家谱网站 MyHeritage 宣布，与该公司的 9200 万个帐户相关的电子邮件地址和密码信息被黑客窃取。

7、 韩国最大虚拟币交易平台被黑，约 2 亿元资产被盗

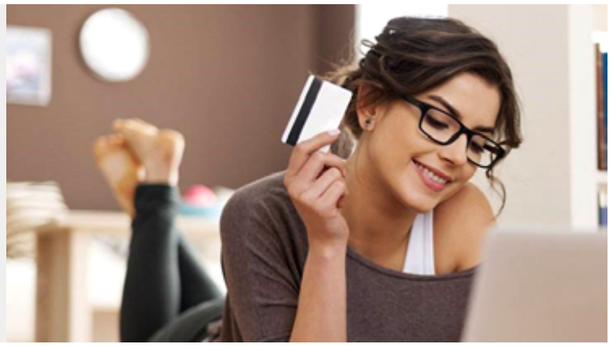
摘要：中新网 6 月 20 日电据韩联社报道，韩国最大虚拟货币交易平台 Bithumb 遭黑客入侵，约 350 亿韩元 (约合人民币 2.04 亿元) 资产被盗。

8、 美国 Uber 因侵犯隐私 20 年内将受监督

摘要：有消息称，近日，Uber 和美国政府达成和解协议，美政府要求 Uber 采取一系列整改措施，另外在未来 20 年内，需有第三方对 Uber 的软件和相关行为进行监督。

9、智利银行被黑：近万台电脑瘫痪，被盗千万美元

摘要：智利银行承认在五月份的黑客攻击中损失大约 1,000 万美元；在这次攻击中，大约 9000 台电脑和服务器的 mbr 被破坏，造成这些设备无法启动。



10、美票务巨头 Ticketfly 遭客勒索比特币 已停业 24 小时

摘要：美国票务巨头 Ticketfly 遭遇黑客攻击勒索，出现了严重的数据泄露，损害了其中一些客户的个人信息。截至目前，公司暂停营业的时间已经超过 24 小时，正在进行全面深入的调查。

访谈 | 从行业需求角度看数据安全


张磊

个人简介

张磊，亿赛通副总经理，负责公司销售线和技术线管理工作，曾担任绿盟科技销售总监，负责中央部委行业销售管理工作。加入绿盟集团之前曾就职于索尼集团索贝数码，负责中央部委行业大客户销售工作。

近两年数据泄露、勒索攻击等安全事件的集中爆发，让“数据安全”领域的热度不断升温。今年 4 月被称作网络安全行业风向标的 RSA 大会上，“数据安全”更是登顶最受关注的安全热词（统计来源：安全牛 RSA2018 热词云图），从安全厂商的角度一定程度印证了这一趋势。再加上欧盟通用数据保护条例（GDPR）今年 5 月 25 日后的正式实施，企业所要承担从合规角度对数据安全的要求会更加严苛。

作为国内最早专注数据安全领域（电子文档安全）的厂商，成立于 2003 年的亿赛通在 2014 年被绿盟科技全资收购，作为后者在数据安全领域重要的能力补足。收购完成后 4 年，仍独立运营的亿赛通如何看待愈加火热的数据安全市场？亿赛通又将如何利用自身已有的优势完善他的销售体系？安全牛记者近期采访了负责亿赛通销售线和技术线的副总经理张磊。

一、事件驱动的数据安全市场

安全牛：为国内最早的一批数据安全厂商，亿赛通在文档加密领域从成立开始到现在已经 15 年了，如何看待国内数据安全市场的发展？

张磊：数据安全的概念比较复杂，覆盖范围广，包括做数据备份、电子文档安全、数据泄露防护、数据库安全、磁盘加密的都可以自称为数据安全厂商。但真正从安全角度来看，我认为，只有囊括了电子文档安全和数据泄漏防护的产品才是最贴合国内需求的。特别是文档加密这个点，在国外都是不常见的，只是作为整体产品能力的一环，不像国内，已经形成了一个相对比较独立的市场。当然现在数据安全这个概念也越来越大，比如亿赛通，除了电子文档安全和 DLP 外，我们也在做大数据安全、数据库审计、UEBA 等解决方案。

国内最早的数据安全市场，是事件驱动起来的。如十几年前某高层内部的讲话泄露事件。那时候，国内还没有其它做加密的厂商，但是亿赛通实际上在这个事件发生前就已经成立，因为提前看到了这样的需求。之后，来自军方、涉密单位类似的需求越来越多，这个市场也慢慢开始热起来。

安全牛：还有一些高科技、制造等企业级市场？

张磊：是的，受“中国制造 2025”纲领的影响，企业对内部核心数据的安全保护需求是非常强的。

比如说亿赛通最早覆盖的“设计、制造、研发、通讯”这四个行业，对于他们来讲，代码、设计图纸是企业最核心的资产，一旦发生数据泄露，企业的核心竞争力就会大减。尤其是芯片的设计和制造，流程和工艺都是非常复杂的，而壁垒形成的关键就在于核心技术的积累，所以他们对知识产权的保护也是做得最到位的。

当然，这里有个大前提，就是企业要明白，安全永远只能是相对的安全。如果是通过超强的记忆力、录音等手段，无论你的防护效果再强，也没有太大效力。所以我们要做的，是让绝大多数人很难以较小的代价轻易获取这些受保护的文档。

安全牛：没错，安全防护的价值很大程度是在于提高攻击门槛，而不是要保证万无一失。亿赛通去年市场营收情况如何？

张磊：我们 2017 年全年营收比 2016 年增加了近一倍，而且电子文档安全这部分也是在大幅增长的。之前有国内的咨询机构估算，亿赛通 2016 年大概占了国内数据泄露防护总市场份额的 20.6%，是这个领域占比最大的厂商。

客户组成方面，目前主要有八个行业，设计、制造、研发、通讯、政府军队军工、金融、运营商和能源电力。这其中，特别是一些有特殊业务系统的政府单位，比如海关、税务、社保、知识产权局等，他们对电子文档加密和 DLP 这两个方面的需求都是有且非常明确的。

二、不同管控手段 不同应用场景

安全牛：作为国内最早做文档加密的厂商，亿赛通的技术优势有哪些？

张磊：我觉得亿赛通和其它友商最根本的区别，或者说最大的优势在于我们的产品是基于驱动层开发，而其他厂商大部分是基于应用层开发的。产品的开发理念和底层开发架构有本质的区别。这种区别在使用过程中，客户会有明显的体会。

还是以研发行业举例，因为研发需要加密的文件普遍比较大，所以基于应用层开发的产品，它的加密效率和成功率都会比较低。要么编译不通过，要么编译时间比基于驱动层的长好几倍。从用户体验来讲，这个差别是非常大的。这也是为什么在这些行业，亿赛通能够拥有近 2/3 市场占有率的核心原因。

当然，基于应用层也有自己的好处，比如软件更加灵活，兼容性强等，这个并不能一棒子打死，各家的产品设计理念是不同的。

安全牛：DLP 有没有可能代替原来的文档加密体系？

张磊：我之前认为有可能，但现在从市场的反馈来看，电子文档加密这个市场在国内还是有很大增长空间的。

很多人对加密的对象有误解，认为加密对象大多是 Word、Excel、PDF 等常见的办公文档，但其实真正的加密对象很多是设计图纸和代码。而且不同行业对文档加密能力的关注点也不太相同。当然，加密的效率，产品的稳定性和兼容性，是所有客户的基础需求。这几点也是最考验厂商技术积累和产品经验的。

以内容识别能力为主的 DLP 和文档加密，可以说本质上是两种不同的数据管控手段。

在金融、互联网等行业，企业的需求会向效率、事后的审计和追责倾斜。比起文档加密这种强管控但是低效的手段，他们选择 DLP 的情况会更多。尤其是互联网这种年轻的行业，员工的法律意识和安全意识都要比传统行业强，一旦发生数据泄露，企业的解决思路更多是诉诸法律手段。结合相关法律，DLP 可以更好的从技术层面帮助企业维权。这有点类似电子取证。这个需求，我们看到今年也开始慢慢起来了。

安全牛：所以说，DLP 和文档加密的不同在于他们的应用场景。

张磊：可以这么认为，同时在某些层面他们是有机融合，而不是一个相互替代的关系。

三、文档加密和 DLP 的融合

安全牛：你认为 DLP 包含文档加密么？

张磊：真正的 DLP，无论是国外或国内，我认为都是不包括加密这部分内容的。但是，在产品层面，这两个能力点又可以融合。

我们在 2016 年就提出了这样一个平台（DSIP），基于亿赛通在电子文档安全、磁盘介质安全、邮件安全、数据库安全以及 DLP 产品线中对语义、行为分析等技术能力的积累，将加密和 DLP 这两个能力在这个平台上合二为一。

安全牛：为什么想要做这样一个平台？

张磊：还是来自客户的真实需求。亿赛通有个重要的客户，之前他们仅在内部流通的红头文件发生了泄露，而恰恰在这个文件中包含了非常敏感的企业战略信息。这个文件泄露后还在网上引发了不小的争论。这个客户就对我们提出了类似的需求：希望有一个产品，既能帮助一些企业内部的敏感部门，保护他们的重要信息，如战略投资数据等，不会被轻易泄露；又能做到事后的审计追踪，提供双重保护。

安全牛：国外虽然也有类似的事件发生，但很少见到厂商推这样的产品，你觉得是为什么？

张磊：首先国外的企业不整合是因为这是不同的产品线，我们整合是因为国内的客户需要这种定制化的数据安全解决方案。

还有就是因为汉语和英语的差别 ，国外 DLP 产品在中国是水土不服的，DLP 来源于国外，初衷是防止无意识泄密的，技术上属于弱管控，比如挂载硬盘这么简单的操作就可以绕开，但是如果把传统 DLP 和磁盘加密结合起来，磁盘加密解决了磁盘非法挂载的安全问题，这样就可以很快速的提高整体的数据安全能力，这也是我们为什么要整合的原因之一。

安全牛：这需要安全咨询在前期配合吧？

张磊：对，一些高端客户，为配合产品的顺利部署，一开始会是咨询先行。通过“诊断”明确问题后，再结合我们的产品，对症下药。只有通过这种“人 + 工具”的模式，安全能力才能真正做到有效且最大化。

安全牛：亿赛通未来的战略方向是怎样的？

张磊：亿赛通现在的市场增速很快，但越是这个时候，我们越要厉兵秣马，要夯实基础，不能一味地往前跑。

如果把亿赛通比作人的话，那么电子文档安全和数据泄漏防护就是“食粮”，这是目前为止亿赛通最强势的主营业务，同时也会加大数据库审计、数据库防火墙、大数据安全、UEBA 等产品线的投入。

四、研发与销售 双轮驱动

安全牛：如何看待亿赛通和绿盟的关系？渠道方面，双方有什么合作？

张磊：2014 年亿赛通被绿盟科技全面收购，作为绿盟科技的全资子公司，经过 4 年的不断融合与发展，目前在销售、研发、技术上的合作流程、合作体系均已健全，为用户提供网络安全、数据安全全方位的信息安全解决方案，双方通力合作全面布局整个信息安全市场，实现了一个共赢的良好局面。

亿赛通目前是完全独立运营的 ,有自己成熟的销售体系。确实，绿盟自身的渠道体系很强大，因此我们把绿盟当做是亿赛通的一个销售渠道。目前，亿赛通的认证签约渠道有百余家，分布几乎覆盖全国。自身有足够技术能力的渠道，我们统一称他们为签约代理商；其余归为合作伙伴。签约代理商在亿赛通的渠道体系里是占了大多数，而且销售份额稳定。

安全牛：为什么这么看重渠道的技术能力？

张磊：因为终端和网络安全产品的销售模式是完全不一样的。终端产品的单点安装、调试，维护起来往往非常耗费人力，所以我们签约的代理商，必须具备相应的技术能力来去做这件事情。当然，我们也会定期帮他们培训、解答一些疑难问题。

安全牛：可以说“销售”是亿赛通的核心驱动力么？

张磊：一半吧，另一半是产品研发。我是销售出身，知道销售在企业中的作用有多重要，所以我自身是比较喜欢销售驱动型的企业的。但到了终端市场，我认为产品研发和销售应该是一半一半。

网络端的安全设备出现了问题后 ,如果工程师不去机房，尤其是旁路部署的，很有可能很长时间用户完全不知情；但终端类的安全产品，即使问题只出了一分钟，客户整个公司的员工就都会知道。虽然酒香也怕巷子深，但是如果自身产品实力不过硬，市场销售能力再强也没戏，反而会砸了自己的牌子。

安全牛：嗯，有道理。销售方面，未来亿赛通有哪些规划？

张磊：对于亿赛通而言，目前最重要的就是做自己，最大的竞争对手也是自己。

可能外界经常拿亿赛通和明朝万达、中软做对比，但如何让我们销售体系内的人员更加规范，技术人员可以很快的完成部署、售前人员有更专业的态度和知识，甚至能够在现场自己就完成小的咨询，让用户更加了解自身的痛点和亿赛通的产品，这才应是我们 2018 年工作的重头戏。

渠道方面，我们始终是把这些签约的渠道代理商也当作自己人来看待。每月，我们都有针对代理商的集训营，他们可以在亿赛通的研发部和项目管理部参加相应的培训课程。

我相信，如果能把销售和技术培养好，把代理商的培训和支持工作做好，让他们强大起来，之后拓展渠道、开拓市场，获得更多的市场份额就都是水到渠成的事情。

安全牛：最后，作为一位优秀的销售，可否分享一些这方面的经验？

张磊：三点吧，第一，也是最基础，就是勤奋和坚持。

我之前是打电话起家，当时还是在广电圈，每天 200 通电话，我打了大概半年时间，认识的客户不超过 10 个。但是，作为新手，找到一个就能让我很高兴。通过维系这为数不多的几个客户，他们再介绍新的客户给我认识，我的圈子也开始慢慢扩大。

第二，是做人。

做销售，一定是先做人。我当时刚毕业，直接接触的客户，大多数是部委单位的处级领导，他们一眼就可以看透你的想法。我的思路就是知无不言，产品好就好，不好就是不好。客户担心的不是你的产品有不足，而是他们不知道哪里有不足，这才是最可怕的。所以当时的态度很诚恳，让客户很放心，互相建立信任感。

第三，就是做事认真、高效、负责。答应什么时候给客户方案、拜访客户，不拖沓、不迟到。

做到这三点，我认为就已经是个合格的销售了。

如果要想做到优秀的话，更重要的是多从客户角度出发，站在客户角度多思考问题，急客户所需、想客户所想，真正的为客户带来周到全面的服务，“用心服务好客户”不是一句口头禅，而是需要用行动去感化，这也是我们销售团队一直努力的方向。

亿赛通全新推出“勒索病毒防护卫士” 为您的数据穿上防弹衣

勒索病毒威胁升级

近 些 年 勒 索 病 毒 频 发，“WannaCry”、"NotPetya"、“坏兔子”，每次勒索病毒的爆发都引起各行各业的恐慌。今年年初，国家网络与信息安全信息通报中心紧急通报：勒索病毒出现变种。病毒主要以国内公共机构服务器为主要攻击对象，多家医院服务器遭到攻击，导致系统瘫痪，数据库文件被加密破坏，已严重影响医院的正常就医秩序。如何有效防止勒索病毒的攻击，已经成为各组织信息安全建设重点关注的课题。

目前市场上常见的勒索病毒防护方案有两种：一是数据备份，在遭到病毒之后可恢复历史文件，却只能挽回少量损失；二是杀毒软件，可发现恶意攻击，但是并不能发现变种勒索病毒。这两种解决方案虽然都能挽回一定损失，却并不能真正防止勒索病毒对文件的破坏。我们更应该思考的是如何从根源彻底防止数据文件被病毒加密。

亿赛通作为国内数据泄露防护领域的第一品牌，针对勒索病毒的防护研究始终在进行中，此次全新推出自主研发的“勒索病毒防护卫士公益版 V1.0”，对数据文件进行保护，使勒索病毒无法对数据进行加密，勒索行为化为泡影。

智能识别全面抵御病毒攻击

亿赛通勒索病毒防护卫士公益版 V1.0：国内首款勒索病毒防护软件，经过专业测试，可主动抵御各种勒索病毒对企业核心文件的攻击加密。软件采用可信进程、进程签名等技术，通过对进程进行智能识别，防止各种勒索病毒软件对用户文档进行恶意加密，从而有效保护

您的数据资产安全。

产品具体功能

1. 智能学习：用户可自主选择需保护目录进行学习，可学习到被保护目录下文件的合法访问进程及文件路径信息；

2. 策略应用：将学习结果生成文件保护策略并应用；

3. 文件防护：支持对文件开启或关闭防护，开启防护后将拒绝非法进程访问被保护目录下的文件；

4. 违规记录：支持记录被拒绝访问的软件进程及拒绝访问的文件及路径；

5. 策略维护：支持将未学习到的合法进程添加到文件保护策略中。

亿赛通——中国数据安全防护专家，坚持从源头上真正的保护用户数据安全，即使勒索软件变种多样，防护卫士均可能做到完美抵御，打击非法勒索黑产，我们一直在路上！

如果您想了解更多产品相关资讯，获取注册方式，请咨询：400-898-1617，我们竭诚为您服务！

亿赛通成为中国国际科技促进会商业秘密保护专业委员会重要成员，与专业机构共建商业秘密全方位保护体系

中国国际科技促进会商业秘密保护专业委员会成立大会暨首届中国新时代商业秘密保护高峰论坛 6 月 9 日在京召开，委员会旨在为促进新时代我国企业商业秘密保护的研究、立法和实务，为企业创新和科技转化保驾护航。亿赛通副总经理张磊作为委员会特聘成员之一出席成立大会，未来公司将携手各大专业机构、事务所、企业共同整合商业秘密保护的管理、法律和信息技术资源。打造商业秘密保护的事前风险防范、事中调查取证、事后维权救济的全方位、立体式的保护机制，帮助企业建立健全商业秘密保护体系，解决企业后顾之忧。

数据安全不再赤手空拳

亿赛通高级咨询顾问以《商业秘密与数据安全结合应用研究》为主题，与到场人员分享目前数据安全市场形式。在企业信息化建设快速发展的前提下，特别是大数据、人工智能等新型信息技术的发展应用，从“熊猫烧香”到“永恒之蓝”，再到苹果公司泄密案，让数据安全已站上风口浪尖。会中，亿赛通充分对商业泄密途径和防护体系进行深度剖析，从“外部入侵”到“内部泄漏”，商业办公环境下存在的数据安全隐患已愈发明显，针对企业数据应做到事前主动防御、事中监测响应、事后追踪溯源，全程态势感知...

此次活动的参与嘉宾还有国际关系学院国际政治系副主任郝敏，北京知识产权法院法官、审判员陈勇、中国网公益中国频道总编辑吴仕鹏、去哪儿网首席运营官胡洁、分享通信副总裁王郁、思科大中华区安全官吴威、天津光电集团有限公司研发中心主任吕前进。华为、京东、滴滴出行、一汽大众、人人车、美团、链家地产、京沃客码头（北京）管理顾问有限公司、绿湾等知名企业有关负责人，以及来自政府有关部门负责人，知名高校专家学者，企业家代表和在京主流媒体记者近两百人出席活动。

随着数据安全市场日渐成熟，用户对于产品性能和稳定性要求越来越高。亿赛通作为数据安全领域领先企业的市场价值也会越来越明显，政策法规也给国内厂商带来了很多机会。公司无论在市场份额、品牌知名度上都一直名列前茅，通过准确把握当前数据安全发展态势，推动数据安全先进技术手段建设，促进专业产品实施应用，越来越受到更多客户的认可。作为专注于 15 年数据安全领域的厂商——亿赛通当仁不让，一直遥遥领先同行厂家，有望在快速增长的安全市场获得更大份额，未来的市场空间将会更巨大。

2018 世界杯正式开幕，严防信息诈骗，别让它成为骗子的狂欢盛宴！

开幕啦，开幕啦，万众期待的俄罗斯世界杯终于在今天正式开幕，对于球迷来说这无疑是一次不容错过的盛会。激情、狂欢、呐喊、疯狂，所有的这些情绪都将随着小小的足球迸发。在全球数百万球迷激动期待的同时，犯罪分子也蠢蠢欲动。

世界杯预热期间，各种诈骗手段就已经随之而来，方式五花八门，都快看这里，看这里，看这里。

1、垃圾信息

不少网友都收到信息和邮件，“世界杯期间赠送 xxx 优惠券”、“送 xxx 粉丝世界杯世界杯纪念旅行抽奖机会”等，并附上链接。网址只要点击进入，手机就会自动被安装上恶意软件。恶意软件会窃取手机里的通话记录，短信记录，位置信息及手机情况等内容。

2、钓鱼网站

想要现场看球又买不到票的球迷们要小心了，很多钓鱼网站声称可以给球迷提供购买门票机会（价格比原价高）。但是，这些门票其实并不能用，并且还会在购买的时候泄露银行账号、身份证号等个人信息。

3、黑客攻击

黑客针对世界杯酒店预订的用户发动攻击。先是攻击了相应酒店，获取了客户的姓名、地址、电话号码、预定日期、价格等详细信息，然后通过手机短信发送虚假消息，告诉他们系统出现了漏洞，需要更改密码。然后，再发送第二条消息，要求全额付款，并告诉用户只有提供银行信息才能进行处理。

4、虚假中奖

在世界杯期间，有很多球迷参与赌球活动，这也给了不法分子机会。他们会像用户发送赌球中奖的短信，并附上链接，只要点击，信息会被全部泄露。更有甚者，制作虚假的博彩网站，引诱球迷上当。

5、世界杯纪念币

除了上述手段，各种打着世界杯旗号销售虚假纪念收藏品的网站也开始增多。 其中又以销售各种虚假纪念币纪念钞最多。在搜索引擎中输入“2018 世界杯纪念币”会发现很多不同域名的小网站在推广销售同类型纪念币。

每遇国际重大事件，这类售卖各种纪念币，纪念钞或纪念邮币的网站都会开始大量冒出。这些网站往往都是通过吹捧权威机构授权，限量版发行，收藏升值空间巨大等噱头，来诱导不明真相的用户花钱购买。

随着赛事日益临近，诈骗分子的行动也愈发频繁，各种诈骗活动即将轮番上场。只有提高安全意识，更谨慎的对待互联网内容和行为才能实现更好的防骗。 为避免被骗，请大家一定注意以下几点：

1、球赛门票请到官方网站购买；

2、不要在陌生发件人的电子邮件或手机短信中随意打开链接及附件；

3、不要购买垃圾邮件中推广的任何产品；

4、不要参与任何网络博彩活动，切忌因为一时刺激或贪图投机利益而参与；

中国数据安全防护专家亿赛通再次提醒大家，虽然看比赛让人热血沸腾，可是不要降低自己的警惕心哦。不能让犯罪分子有机可乘，他们等的就是你放松的那一刻！

Hold 住！“刘明炜”准考证又丢啦？各大高考诈骗卷土重来，到底该如何防范？

一年一度的高考季又到了，

近些天在微信朋友圈里疯传的是考生考前准考证丢失，

当小编看到这条信息的时候，感觉似曾见过！

话说回来，高考可是人生大事呀！

考生们为了这事准备了 12 年呀！

如果因为准考证丢了错过就还得等一年呀！

小编赶快动动手指转发！转发！转发！

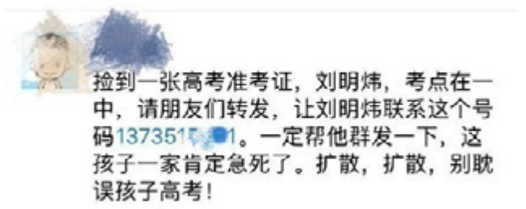
之后就收到多位好友提醒，这是假的！

再上网一查，竟然发现全国各地

叫“刘明炜”的人都丢高考准考证

考点都是一中

只是电话换成了 137XXXXXXXX



在每年的高考季里，总有一些信息让人“牵肠挂肚”，考验人们的心里底线。广大网友出于好心，往往会随手帮忙转发，这样很可能会落入骗子的圈套。在谣言帖子中所留下的考生电话号码可能为吸费电话，打过去就会产生高额通话费用。还有骗子用此来做宣传广告或者干脆直接行骗。更有甚者可能拿别人的号码来恶搞骚扰，给别人的生活造成困扰。

除了这类陷阱，还有很多骗局，那么，高考前后，还有哪些骗局呢？小编给大家一一汇总，一起来看看，避免在忧心忡忡或高度紧张的状态下，误入谣言陷阱哦！

骗局一：提前查分

钓鱼网站会伪装成高考成绩查询网页大面积推广，骗子以“提前查分”为名向考生和家长收取预付金，或用发送病毒的方式感染考生电脑，盗取手机号、身份证号、银行卡号等资料，进而盗取考生的网络支付账号实施诈骗。

亿赛通温馨提示:查分时间和渠道都以官方消息为准，即考生所在省教育考试院，可登录其网站或官方微信等进行查询。

骗局二：出售高考试题

不法分子会发出“出售高考试题”“考题泄露”“专家组押题猜题”等带有链接的虚假信息，诱骗学生和家长购买。

亿赛通温馨提示：不要存在侥幸心理在网上购买所谓的高考试题，给犯罪分子可乘之机。同时，购买考题答案本身也涉嫌违法，切勿尝试。

骗局三：谎称有“内部指标”

不法分子冒充学校招生人员等特殊身份或假装有“内部关系”来骗取家长信任，随后再谎称可通过交钱换取“内部指标”“特殊待遇”等实施诈骗。

亿赛通温馨提示：高考招生有严格的程序和规定，没有“内部招生名额”的说法。

骗局四：高考“抢手”

骗子通过 QQ 谎称自己可以当“高考枪手”，央视也曝光高考枪手替考利益链，给枪手 5 万元可考上重点本科。

亿赛通温馨提示：教育部统一规定对于参加高考替考的“枪手”学生，一律按规定严肃处理；涉嫌犯罪的，移送司法机关追究法律责任。

骗局五：低分可“跳档”录取

每年成绩公布后，都会有人自称有办法让不够一本线的考生录取到一本院校，不到本科分数线的能录取到本科院校。

亿赛通温馨提示：

高考统一为电脑提档，如考生分数不到提档线，无法提档！

骗局六：伪造录取通知书

不法分子通过邮局，向考生寄送伪造的录取通知书，让考生将学杂费打入银行账户内。

亿赛通温馨提示：具体录取信息以教育部官方网站查询的信息或学校统一通知的信息为准，切勿相信自身没有报考的院校所投递来的录取通知书。

骗局七：提前告知录取结果

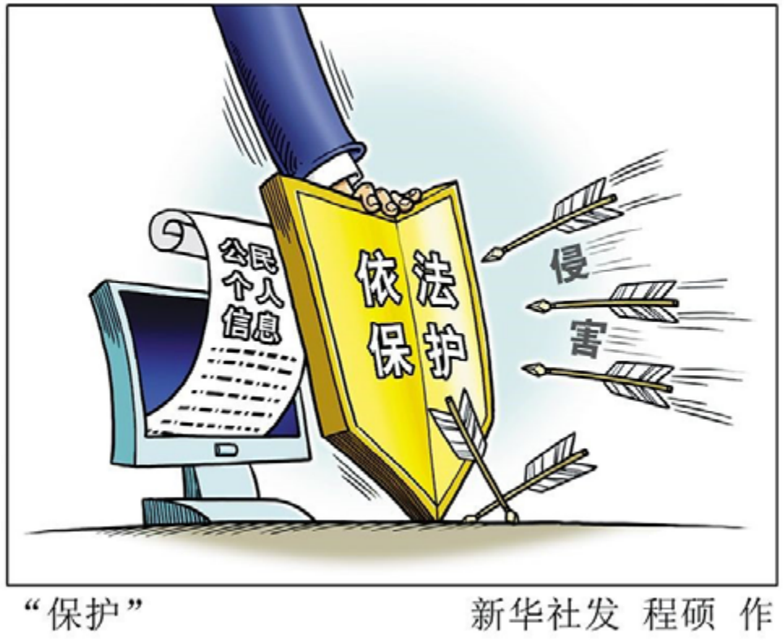
利用考生及家长不熟悉招生程序，不法分子鼓吹自己“上面有人”“保证录取”，公开叫价。

亿赛通温馨提示：考生及家长应该以本地教育部门官方网站或者报考院校的官网网站公布的录取信息为准，切勿听信提前获取的谣言。

顺便科普

互联网正在飞速发展，各类诈骗手段防不胜防，大家必须加强个人信息保护意识，辨别各种诈骗手段。同时，各教育局、学校、考生及家长也必须高度重视，注意保护好考生个人信息，不要让不法分子有机可乘，避免对学生造成极大伤害。国家也高度重视考生信息防护，杜绝信息泄露。亿赛通作为专业的数据安全防护专家，一定肩负起信息安全保护的责任，全力支持各相关单位共同倡导大家加强防护意识，保护好学生信息。

各大法规陆续实施，这些条文你具体了解多少？



2018 年从年初开始，各类数据泄露事件接连发生，国家对信息安全愈发关注。不管是国际还是国内，对于个人信息安全的保护正处于缰绳越收越紧的状态，接连实施了多个法律条文，保障信息安全、维护社会公共利益、保护公民、法人和其他组织的合法权益。对此，亿赛通特从专业的角度，为您详细解读您必须了解的法律相关内容。

快递暂行条例

2018 年 5 月 1 日起实施

隐私保护 泄露寄件人隐私最高罚款 10 万元

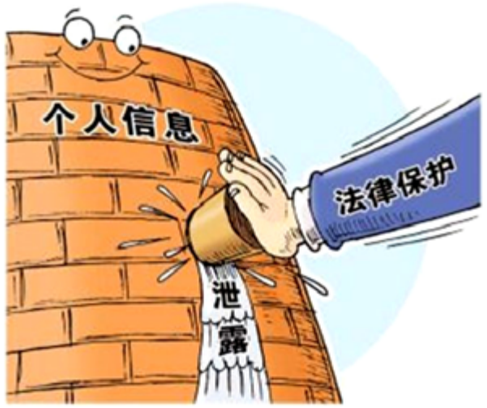
第四十四条：经营快递业务的企业有下列行为之一的，由邮政管理部门责令改正，没收违法所得，并处 1 万元以上 5 万元以下的罚款；情节严重的，并处 5 万元以上 10 万元以下的罚款，并可以责令停业整顿直至吊销其快递业务经营许可证：

（一）未按照规定建立快递运单及电子数据管理制度；

（二）未定期销毁快递运单；

（三）出售、泄露或者非法提供快递服务过程中知悉的用户信息；

（四）发生或者可能发生用户信息泄露的情况，未立即采取补救措施，或者未向所在地邮政管理部门报告。



个人信息安全规范

2018 年 5 月 1 日起正式实施

《规范》明确了“敏感个人信息”的范畴。《规范》及其附录确定了敏感个人信息的认定标准、实例以及敏感个人信息的特殊合规要。

亮点一：不得欺诈、诱骗、强迫个人信息主体提供其个人信息；不得隐瞒产品或服务所具有的收集个人信息的功能；不得从非法渠道获取个人信息；不得收集法律法规明令禁止收集的个人信息；

亮点二：收集的个人信息的类型应与实现产品或服务的业务功能有直接关联；自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量；

亮点三：收集个人信息前，应向个人信息主体明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则（例如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等），并获得个人信息主体的授权同意；

亮点四：应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；

亮点五：应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露等；

亮点六：收集个人敏感信息时，应取得个人信息主体的明示同意。应确保个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的愿望表示；

亮点七：向个人信息主体告知所提供产品或服务的核心业务功能及所必需收集的个人敏感信息，并明确告知拒绝提供或拒绝同意将带来的影响。应允许个人信息主体选择是否提供或同意自动采集；

亮点八：产品或服务如提供其他附加功能，需要收集个人敏感信息时，收集前应向个人信息主体逐一说明个人敏感信息为完成何种附加功能所必需，并允许个人信息主体逐项选择是否提供或同意自动采集个人敏感信息；

亮点九：收集年满 14 的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意；

亮点十：个人信息保存期限应为实现目的所必需的最短时间；超出上述个人信息保存期限后，应对个人信息进行删除或匿名化处理；

亮点十一：收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信息处理中不重新识别个人。

GDPR 通用数据保护条例

2018 年 5 月 25 日起正式实施

GDPR 适用于在欧盟境内没有业务机构的组织，28 个成员国，大约有 5 亿多人可以直接得到 GDPR 的保护。对违法企业的罚金最高可达 2000 万欧元（约合 1.5 亿元人民币）或者其全球营业额的 4%，以高者为准。

1、对涉及到数据主体的个人数据，应当以合法的、合理的和透明的方式来进行处理；

2、个人数据的收集应当具有具体的、清晰的和正当的目的，对个人数据的处理不应当违反初始目的；

3、因为公共利益、科学或历史研究或统计目的而进一步处理数据，不视为违反初始目的；

4、个人数据的处理应当是为了实现数据处理目的而适当的、相关的和必要的；

5、个人数据应当是准确的，如有必要，必须及时更新；

6、必须采取合理措施确保不准确的个人数据，即违反初始目的的个人数据，及时得到擦除或更正；

7、对于能够识别数据主体的个人数据，其储存时间不得超过实现其处理目的所必需的时间；超过此期限的数据处理只有在如下情况下才能被允许：为了实现公共利益、科学或历史研究目的或统计目的，为了保障数据主体的权利和自由，并采取了合理技术与组织措施；

8、 处理过程中应确保个人数据的安全，采取合理的技术手段、组织措施，避免数据未经授权即被处理或遭到非法处理，避免数据发生意外毁损或灭失；

9、数据主体可以要求控制者提供对个人数据的访问、更正或擦除，或者限制或反对相关处理的权利；

10、数据主体拥有可以随时撤回——这种撤回不会影响撤回之前根据同意而进行处理的合法性——同意的权利。

在这个“蹭吃”、“蹭喝”、“蹭 WIFI”的时代，黑客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。

亿赛通与南通中集达成战略合作意向，提升企业数据安全管理能力

客户简介

南通中集罐式储运设备制造有限公司成立于 1998 年，公司作为中集集团的重点企业、中集安瑞科能源化工食品装备板块骨干企业，专业从事能源、化工食品装备行业的化学品物流装备、气体能源储运装备、化工过程装备和核能源装备等设计与制造业务。公司资产 20 亿元，员工 3000 人，具有标准罐箱、特种罐箱、压力容器、高压气瓶、核电与重型化工装备八条生产线、近 20 个产品线的近百个产品品种，是目前全球规模最大的罐式集装箱生产厂家。

需求背景

南通中集公司作为行业的领军企业，为了防止企业内部的研发设计图纸、财务、市场等部门的重要资料在无任何防护措施的情况下被内部员工泄露、被竞争对手窃取，从而影响南通中集在行业中的竞争力，因而启动了数据安全管理项目。

亿赛通对南通中集的网络环境现状进行了充分调研和论证，设计出完善的解决方案，经过测试，在多家数据安全厂商中脱颖而出，南通中集决定选择亿赛通对其数据安全体系保驾护航。

解决方案

电子文档安全管理系统实现内部透明，用户使用无感知；外部用户非法获取内部文档无法使用；合法用户获取内部加密文档按权限使用。

1、文档透明加密

根据文档的类型进行自定义，对应类型的文件自动进行加密处理。

2、文档外发管理

外发文档提供细粒度权限控制保护，包含文档使用权限如只读、打印、修改等控制；文档生命周期管理如：阅读次数、阅读时限及过期自动销毁等保护；文档协同权限如修改、还原以及文档内容保护、打印水印等控制。

3、内容防护

为防止使用者恶意将文件内容扩散，系统对其内容进行高强度安全控制，如内容剪切保护、禁止截屏、禁止另存为及打印控制等。

项目成果

在部署电子文档安全管理系统后，南通中集罐式储运设备制造有限公司庞大的工作业务系统数据得到优化管理，无论其内部、外部威胁环境都无法窃取企业敏感的核心数据，让公司所有员工都能够高效的进行安全工作。

中国数据安全防护专家亿赛通，连续 15 年领跑中国数据安全管理市场，接下来将继续肩负“保护数据所有者信息资产安全”的使命，保持创新技术、优质服务、开放合作的传统优势，继续引领数据安全市场前行。

亿赛通签约北京市劳动和社会保障局

客户简介

根据中共中央、国务院批准的《北京市党政机构改革方案》，设置北京市劳动和社会保障局（简称市劳动保障局）负责本市劳动和社会保障行政事务的市政府组成部门。

典型案例 TYPICAL CASES

需求背景

市劳动保障局负责根据国家劳动和社会保险法律、法规，起草劳动和社会保险方面的地方性法规、规章草案，制定劳动规范和基本标准并组织实施，以及管理社会劳动力，组织建立、健全就业服务体系等任务，由于涉及大量国家政策重要信息，为了避免信息随意泄露、外传，因此需要加强对涉密信息的安全管理。

解决方案

全盘加密安全 U 盘，为客户提供以下解决方案：

进不来：非法用户无法登陆 U 盘系统进行控制使用；

拿不走：非法用户通过任何手段或底层暴力破解，都无法获得 U 盘加密区的数据信息内容；

读不懂：U 盘加密内数据全部密文存储、非法用户无法识别；

走不脱：U 盘具备日志审计功能，对操作行为可记录和追踪。

项目成果

继打造了坚固的安全 U 盘管理系统后，有效的保障了市劳动保障局涉密信息的安全。