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

06 月刊

2017 年共 11 期

新一轮 Petya 病毒全球迅速蔓延 亿赛通 & 绿盟科技携手

跨越古都“西安”共同扼杀新病毒 打造智慧安全 2.0

关注企业官方微信

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

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：86-10-57933888

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS 目录

刊首语 PREFACE

2/3 刊首语

行业聚焦 INDUSTRY FOCUS

4-7 《网络安全法》实施：实现网络安全的法治保障

8/9 别让智能设备成为网络安全的“蚁穴”

10 投资逾 5 亿澳元 澳 CEO 比全球同行更担心网络安全

11 共和党合作数据公司意外泄漏近 2 亿美国选民的个人资料

亿赛通动态 ESAFENET NEWS

12/13 赛迪权威报告 亿赛通数据安全市场份额持续稳居前列

14/15 中国“智”造 全新活力 亿赛通出席 2017 宁波“互联网 + 智能制造”产业发展高峰论坛

16/17 亿赛通再次携手绿盟科技出席“智慧安全 2.0”南京站巡讲活动 共同构建智能安全

18/19 新一轮 Petya 病毒全球迅速蔓延 亿赛通 & 绿盟科技携手跨越古都“西安” 共同扼杀新病毒 打造智慧安全 2.0

亿赛通小贴士 ESAFENET PROMPT

20/21 《网络安全法》6 月 1 日正式实施 7 章 79 条内容 5 大亮点与你我息息相关

22/23 U 盘“替身”病毒正在全国范围内大量交叉感染 毕业季论文是关键 呼叫大神有招吗？

24/25 高考之后招生诈骗案件进入了活跃期 如何识破这些“诈骗”手段？

26-29 不要比特币 亿赛通帮您恢复被勒索加密的数据资产

典型案例 TYPICAL CASES

30/31 制造业深度融合互联网新发展模式 亿赛通协同推进“中国制造 2025”保障数据安全

32/33 亿赛通 DLP 提升中集集团等级管理建设能力 助力企业实现智能化数据安全防护体系

34/35 亿赛通智能感知中国石油敏感数据 助力公司实现内网综合一体化防护

六月刊
带您一同领略诈骗大招数

六月的阳光隐藏着它的威力，一年一度的全国高考成为众多莘莘学子和家长期待而又紧张的时刻。因为，高考，是通往象牙塔的必经之路；高考，是十二年寒暑交替苦读的结果；高考，是个人人生的分水岭……虽然，高考距离很多人已经成为过去，但是每年的高考都会调起我们的回忆，苦涩后的甜美，犹如嚼橄榄的味道，是战地黄花别样香的自豪！

想到高考结束后，所有学生进入完全放松状态之后的激动不已，但却不得不提醒所有参加高考的学生和家长，根据往年经验，每年高考之后，形形色色的招生诈骗案件进入了活跃期，家长心中的急切、侥幸甚至是上当受骗后碍于面子不愿声张的心态，都成了骗子们手中的小尾巴。6月1日，中国第一部网络安全的专门性综合法律《网络安全法》正式实施，此法的实施对于保障网络安全、维护网络空间主权和国家安全、社会公共利益、保护公民、法人和其他组织的合法权益具有十分重要的意义。那么，如何识破“诈骗手段”？本月数据安全行业发生了哪些大事件？请走进亿赛通六月刊，一起领略诈骗大招数……

《网络安全法》实施：实现网络安全的法治保障

源于我国面临国内外网络安全形势的客观实际和紧迫需要，2016 年 11 月 7 日，《中华人民共和国网络安全法》（以下简称“网安法”）经第十二届全国人大常委会第二十四次会议表决通过，已于 2017 年 6 月 1 日施行。网安法为我国有效应对网络安全威胁和风险、全方位保障网络安全提供了上位法依据。法律的生命力在于实施，在网安法正式生效前，Wannacry 勒索软件攻击事件再次给我国网络安全法律治理敲响了警钟，进一步彰显了法律实施的紧迫性和必要性。

一、战略发布：不断强化网安法提出的原则和政策

2016 年 12 月 27 日发布的《国家网络空间安全战略》，是我国首次发布关于网络空间安全的战略。战略与网安法提出的构建网络空间的“和平、安全、开放、合作”原则相衔接，从国家战略层面诠释了网安法主张的网络空间主权原则，将“坚定捍卫网络空间主权”作为九大战略任务之首，强调“根据宪法和法律法规管理我国主权范围内的网络活动，保护我国信息设施和信息资源安全，采取包括经济、行政、科技、法律、外交、军事等一切措施，坚定不移地维护我国网络空间主权。坚决反对通过网络颠覆我国国家政权、破坏我国国家主权的一切行为”；战略将“保护关键信息基础设施”作为九大战略任务之三，进一步拓展了关键信息基础设施的外延，将重要互联网应用系统纳入其中，强调着眼识别、防护、检测、预警、响应、处置等环节，建立实施关键信息基础设施保护制度；同时，战略再次强调要建立实施网络安全审查制度，加强供应链安全管理。

2017 年 3 月 1 日发布的《网络空间国际合作战略》，全面宣示了我国在国际互联网治理问题上的基本原则和行动要点，奠定了我国在国际社会竞争中的话语权和软实力。该战略站在各国共同维护网络空间安全的角度，重申了网安法的和平、主权原则；战略主张的“促进企业提高数据安全保护意识，支持企业加强行业自律，就网络空间个人信息保护最佳实践展开讨论。推动政府和企业加强合作，共同保护网络空间个人隐私”的行动倡议与网安法第四章“网络信息安全”的个人信息保护规定紧密契合。

这两个战略开启了我国网络空间治理的全新范式，巩固和强化了网安法构建的由内而外、自上到下的原则和政策，为我国网络安全相关政策和配套法律的出台指明了方向，有助于继续深入推进网络主权保障、关键信息基础设施保护、个人信息保护、国家安全审查等方面的法律构建。

二、配套规定出台：有效衔接网安法构筑的制度和规则

网安法从运行安全、信息安全和事件应对三个维度立体化、全方位保护网络安全。相关部门正制定或出台相应的下位法与之配套，切实保障网安法的可操作性，避免流于表面化。

在网络运行安全方面，网络安全审查和关键信息基础设施保护制度是下位法制定的重点。网安法第 35 条规定应该对可能影响国家安全的关键信息基础设施的网络产品和服务进行国家安全审查，该条已在国家互联网信息办公室 2017 年 5 月 2 日发布的《网络产品和服务安全审查办法（试行）》中进行了具体规定，该规定是首个正式生效的网安法重要配套规定，并已于 6 月 1 日同步施行。该办法旨在提高网络产品和服务安全可控水平，防范供应链安全风险。根据该办法，关系国家安全和公共利益的信息系统使用的重要网络产品和服务以及关键信息基础设施运营者采购的网络产品和服务，可能影响国家安全的，都要经过网络安全审查；网络安全审查重点在于网络产品和服务的安全性、可控性。

信息安全等级保护制度是国家对基础信息网络和重要信息系统实施重点保护的关键措施。我国的信息安全等级保护工作初步实现了标准化、规范化，但是仍呈现体系不完善、重点不突出、保护效果不佳、保护对象不完整等问题。网安法第 21 条提出国家实行网络安全等级保护制度，第 31 条进一步要求关键信息基础设施要落实国家安全等级保护制度，突出保护重点，是深化信息安全等级保护制度、保护国家关键信息基础设施和大数据安全的迫切需要。为落实网安法第 21 条和第 31 条的规定，必须科学合理地推动网络安全等级保护制度的演进与变革，构建和完善等级保护 2.0 制度体系。

网安法第 31 条规定建立关键信息基础设施保护制度，授权国务院制定关键信息基础设施的具体范围和安全保护办法。关键信息基础设施安全保护办法是法律中唯一明确规定“由国务院制定”的行政法规，也是网络安全法律体系的重中之重。主管部门已开展了相关条例的具体调研、安全检查、起草编写、部门论证和企业座谈等工作。在与关键信息基础设施保护配套的强制性标准方面，全国信安

行业聚焦 INDUSTRY FOCUS

标委 2017 年工作重点之一即为落实网安法要求，加快推动重点标准研制，网络安全产品与服务、关键信息基础设施保护等强制性国家标准的研究。由此可见，与网安法第 31 条配套的法规、国家标准等正在经历着缜密的夯实历程。

网安法第 37 条首次在法律中确立了对个人信息及重要数据出境的安全评估制度，并授权国家网信部门会同其他监管部门制定详细的安全评估实施办法。数据本地化属于境内外实体的重大关切，《个人信息和重要数据出境安全评估办法（征求意见稿）》已于 5 月 11 日结束公开征求意见。评估办法以《国家安全法》和《网络安全法》等为上位法依据，扩大了数据本地化及安全评估义务适用对象的范围，解释了重要数据的概念，数据评估的重点内容，不得出境的条件等，正式制度出台和具体实施有待在实践中进一步观察。

在网络信息安全方面，《互联网新闻信息服务管理规定》也于 6 月 1 日同步施行，规定第 13 条第一款和十六条第二款分别衔接了网安法第 24 条用户身份管理制度的要求和第 47 条处置违法信息的义务要求，互联网新闻信息服务提供者违反这两款的适用网安法的行政处罚。

两高《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（《解释》）5 月 10 日正式发布，解释降低入罪门槛，严惩侵犯公民个人信息犯罪。在个人信息保护基本立法暂时缺位的情况下，《解释》及时弥补了个人信息刑事责任追责的短板，并实质性的构成了网安法行刑衔接的进一步配套和细化制度，为基本立法提供了案例素材，有利于立法的精准、充分。

三、国际立法变革：网安法后续制度落地的参考方向

国际网络安全相关战略和立法迅速进行改革，美欧纷纷建立全方位、更立体、更具弹性与前瞻性的网络安全立法体系。鉴于事件驱动重大立法规律的存在，可以预见的是，国际立法变革将一直持续。

美国接连通过多部网络安全战略及立法，以加强美国网络安全和抵御网络攻击的能力，如 2016 年通过《信息自由法案促进法》、“应对重大网络攻击最新政策指令”、“安全漏洞披露政策”、《波特曼 - 墨菲反宣传法案》，2017 年通过《国家网络事件响应计划（NCIRP）》、《2017NIST 网络安全框架、评估和审查法案》（NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017）（H.R.1224）等。5 月 11 日，美国总统特朗普签署了《关于加强联邦网络和关键基础设施网络安全的总统行政令》，要求美国采取一系列措施来增强联邦政府、关键基础设施和国家这三个领域的网络安全，明确要求联邦机构必须遵守 NIST 的网络安全框架。欧盟 2016 年 7 月通过第一部网络安全法案《网络与信息系统安全指令》，致力于在欧盟范围内实现统一的、高水平的网络与信息系统安全，欧盟成员国必须在 21 个月内将其转化为国内法，11 月发布了三个有关欧盟《一般数据保护条例》内容的指南，为落实《一般数据保护条例》提供更详尽的指引。英国 2016 年底颁布史上最严协助执法法《调查权法案》，旨在进一步理清执法机构在通信及通信数据拦截、获取、留存及设备干扰等方面的权力，帮助执法机构调查犯罪和防控恐怖主义。

从制度设计层面来看，网安法规定了近 20 项制度，其中，网络安全等级保护制度、网络信息内容管理、网络安全教育和培训、个人信息保护等制度较为成熟，网络关键设备和网络安全专用产品认证、漏洞等网络安全信息发布、关键信息基础设施保护制度、数据留存和协助执法制度、境外网络攻击制裁等更多的制度亟需完善设计和后续落地，在制度的贯彻实施过程中必然存在各种挑战和问题。

而恰恰国际立法变革的内容可以为我国网安法后续制度落地提供参考方向。如美国 2016 年应对重大网络攻击最新政策指令公布了对网络攻击严重程度进行定性的标准，从 0 级到 5 级共分 6 个层次，分别是基准、低、中、高、严重和紧急，其中 3 级及以上被视为“重大网络事件”，将触发政策指令中的威胁应对、资产应对和情报支持活动等反应机制，可以为我国网络安全事件应急处置和境外攻击制裁制度落地提供参考。美国国防部“安全漏洞披露政策”可以为漏洞等网络安全信息发布和漏洞的合法挖掘、合理披露制度构建提供参考。美国《2017NIST 网络安全框架、评估和审查法案》则可为关键信息基础设施保护办法、关键信息技术保护安全要求方面的国家强制性标准制定提供参考。英国《调查权法案》涉及面广，规定细致，可以为数据存留和协助执法制度的完善提供参考等。必须强调的是，相关制度借鉴应考虑其制定和实施的特殊场景，不能照搬国外经验，需根据国情实施本土化改造。

作为我国第一部网络安全管理的基础性保障法，其全面落地实施是网络空间法治建设的重要里程碑事件。网安法以发现、消除网络安全威胁和风险，提升恢复能力为轴心，构建了“防御、控制与惩治”三位一体的立法架构，其配套制度的制定与出台正不断夯实丰满这一立法架构。为降低网安法全面落地实施的难度，网安法配套制度的制定与出台仍需严谨、审慎论证。（公安部第三研究所副研究员 黄道丽）

别让智能设备成为网络安全的“蚁穴”

6 月 18 日，央视曝光了家用摄像头安全隐患，称大量家庭摄像头 IP 地址遭到扫描软件破解，这些非法扫描软件交易已形成产业链。

根据国家互联网应急中心调查了市场占有率排名前五的智能摄像头品牌中的两个品牌，发现仅这两个品牌的摄像头就存在十几万个弱口令漏洞。国家质检总局官网发布关于智能摄像头的质量安全的风险警示称，已检测的 40 批次中，32 批次样品存在质量安全隐患，可能导致用户监控视频被泄露，或智能摄像头被恶意控制等危害。

智能电子设备的快速发展，让摄像头等智能设备的价格和使用方法越来越亲民。对于那些需要照看老人、小孩、宠物，或者想要防盗防灾的家庭来说，装一个摄像头，确实是个看上去不错的选择。然而，摄像头“漏洞百出”，却让这些私人摄像头的使用者，随时存在个人隐私被泄露的风险。

其实，监控平台弱口令漏洞是世界性的问题。“口令”相当于门钥匙，“弱口令”意味着把钥匙放在了外人很容易找到的地方。2014 年，俄罗斯一网站就曾利用安全漏洞入侵英国部分居民的家庭网络摄像头，并将影像信息放到网站上共人随意浏览，使数以百计英国用户的生活“被直播”。

这样的漏洞还可能带来比隐私泄露更广泛的影响。正所谓“千里之堤溃于蚁穴”，去年，恶意代码“Mirai”就利用网络摄像设备的弱口令等安全漏洞实施入侵，造成超过半数美国人无法上网。

当下，智能装备在互联网 + 的时代背景下，促成了生产生活方式的大变革。智能设备的种类越来越多，在逐渐渗入千家万户的同时，其覆盖面不仅包括移动互联网行业，还涉及工业制造、农业生产、医疗教育等各个领域。一旦智能设备漏洞百出，其波及面将不止于家庭，更将影响整个社会的运行。

在技术发展日新月异，全民掀起创新热潮的今天，任何一项创新技术，都应当有成熟的相关技术进行配套，有完善的设施设备加以保障，在满足新技术先进性的同时，保证新技术的可靠性、可行性、适用性，有效控制新技术带来的风险，避免出现安全保障设备反成安全隐患的尴尬局面。

技术产品在走向市场前，质量监督部门要跟上“互联网 +”的发展趋势，将网络安全纳入智能产品质量标准之中，制定明晰的标准细则，将智能系统的普遍漏洞和“低级错误”扼杀在“摇篮”中。

同时，使用智能产品的消费者，需要提升科技素养和安全意识，如在购买摄像头等智能产品时，详细了解摄像头的网络安全性能，尽量避免因技术或个人信息储存不当等原因造成损失。倘若出现问题，则依靠技术和法律手段维护自身权益。

安全是发展的前提，发展是安全的保障。对于智能设备的发展来说，这条规律同样适用。提升智能设备的安全，需要政府、企业、社会组织、广大网民各司其职，各出其力。网络安全之堤，同样需要全社会共筑。（新闻来源：科学网）

投资逾 5 亿澳元 澳 CEO 比全球同行更担心网络安全

据澳洲网报道，毕马威 (KPMG) 会计事务所最新《全球首席执行官展望》报告显示，澳大利亚的顶级首席执行官们比全球同行更担忧网络安全问题。

毕马威报告显示，71% 的澳大利亚首席执行官会将超过 5 亿澳元的营业额用于网络安全投资上，相较之下，全球首席执行官的比例仅为 53%。

毕马威澳大利亚网络安全服务合作人阿奇博尔德对比表示，该结果符合《ASX 100 网络健康检查》报告的结果。这份报告发现，澳大利亚最顶级的企业高管普遍对网络威胁具有高度风险意识。

“网络威胁成为澳洲首席执行官最关注的问题，部分是由于这些网络漏洞对企业造成的巨大影响。”阿奇博尔德称，“以前网络安全问题曾被看做是技术风险，陷入现在已被定义为商业风险。同时还有声誉风险以及它对股东价值和运营可用性的影响。”（新闻来源：中国新闻网）

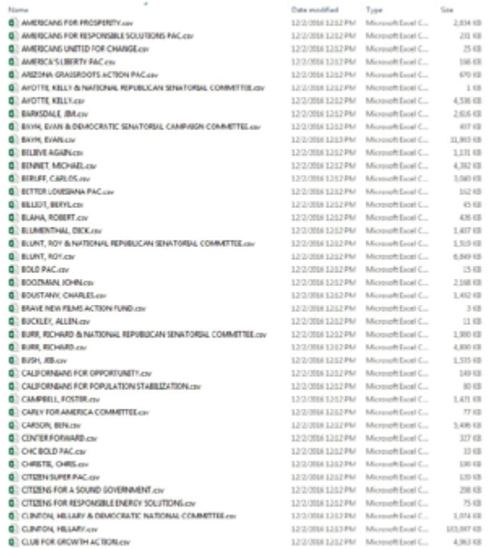
行业聚焦 INDUSTRY FOCUS

共和党合作数据公司意外泄漏近 2 亿美国选民的个人资料

在共和党国家委员会签约的一家营销公司本月泄漏了超过 1.98 亿美国公民的政治数据。数据泄露包含大约 61% 的美国人大量个人信息。除了家庭地址，出生日期和电话号码之外，这些记录还包括政治团体采用的先进情绪分析来预测个人选民如何处理热门问题 ,如枪支所有权，干细胞研究和堕胎权，以及宗教信仰和种族。

Deep Root Analytics 是一个共和党的数据公司供应商，用于确定政治广告的受众群体。UpGuard 网络风险分析师 Chris Vickery 上周在线发现了这些数据。超过 1TB 的存储在云服务器上，无需保护密码，任何人可以访问，这引起了重大的隐私问题，这对有恶意目的的人来说是有价值的。

根据联邦选举委员会的报告，RNC 根据联邦选举委员会的报告 ,支付了 Deep Root Analytics 983,000 美元，但其服务器包含来自各种其他保守方面的记录，其中包括数据信托（也称为 GOP 数据信托），共和党的主要投票者文件提供者。根据 OpenSecrets.org 的数据，Deep



Root Analytics 在 2016 年期间从 RNC 收到了 670 万美元，而其总裁 Johnny DeStefano 则担任特朗普的总统人事总监。（新闻稿源：cnBeta.COM）

赛迪权威报告 亿赛通数据安全市场份额持续稳居前列

近日，由 IT 行业权威媒体赛迪顾问股份有限公司研究统计出《2016——2017 中国网络信息安全市场研究年度报告》。报告详细的介绍了近两年全球数据安全行业的发展现状、市场具体情况、中国数据安全行业具体发展现状、市场情况、以及未来几年之内的发展趋势预测。其中，赛迪报告通过调查、研究得出：2016 年，全球安全服务市场份额最大，达到 1391.7 亿美元，同比增长 12.1%，而中国网络信息安全市场达到了 336.2 亿元，比 2015 年增长 21.5%。从安全市场行业的发展状况能够反映出，安全市场行业的竞争相当激烈。那么，亿赛通从 03 年创立，14 年的品牌铸造，以钻研、专注的态度深耕数据安全市场，坚持服务各大行业，在激烈的竞争状态下坚持本真，稳定发展。在本次赛迪报告的研究、调查对比下，亿赛通在 2016——2017 年度，以 7.1% 的市场份额继续稳居国内数据安全市场前茅位置，品牌影响力范围之广、产品美誉度极高，在行业内被广泛的认可和赞同。

安全服务市场规模达 37.4 亿元 亿赛通全力服务安全市场

2016 年，信息安全事件此起彼伏，对此，人们对网络安全市场的关注度也不断提高，同时也引起了国家对网络安全问题的高度重视，最终让《网络安全法》经过几度的探讨提上法律的条文，并且于 2017 年 6 月 1 日正式实施了此法。在赛迪 2016——2017 年度报告的结果显示中，国内安全服务的市场规模达到 37.4 亿元，安全硬件和安全软件在市场中所占比例仍然最多。亿赛通作为中国数据安全防护专家，发扬持续创新的精神，以产品、方案、服务三个方向为主导，构建了终端数据防护、网络数据防护、应用数据防护、存储数据防护和介质数据防护五大产品体系，涵盖了终端、网络、存储、审计等多个方面的数据安全软硬件产品，为数据安全行业持续提供核心技术保障，其软硬件产品在数据安全市场中占有极大的比重，并且仍在持续的发展壮大中。

品牌云集 亿赛通品牌打响各大区域稳居市场前列

同时，从本次的赛迪报告中，我们看到近年来，国内数据安全市场销售额在华南、华北、东北、西南、西北、华中、华东七大片区中，华北、华南、华东市场销售额比重居多，需求量较大，数据安全需求意识强烈。那么，2016 年，亿赛通在销售渠道方面，覆盖了不同行业和区域的空白区，将市场分别扩展到华南、华北、东北、西南、西北、华中、华东七大区域，华北、华南、华中、华东是亿赛通销售的主力市场，销售份额居多，同时满足七大区域各大行业如军政单位、金融行业、设计 / 制造业、能源行业、运营商、教育行业、医疗行业、交通行业等等的市场需求，将亿赛通品牌和产品打响每一个角落，服务更多的企业保护好自己的数据资产。所以，通过赛迪专家的调查和分析，在 2016——2017 年度，亿赛通保持稳定的增长，在国内厂商份额中，以 7.1% 的市场份额继续稳居数据安全市场前茅之位，并对行业有着极大的贡献意义和价值。

“数据安全” 是一个持续热议的话题，在当下互联网、大数据、人工智能、云计算等各种新的发展时代背景下，安全市场的规模将会持续增大，亿赛通结合新趋势，将会研发出更加符合市场需求的智能化产品、提供智能化的解决方案，帮助企业实现智能化数据安全管控，保护数据资产安全。

活动会议 | 中国“智”造 全新活力 亿赛通出席 2017 宁波“互联网 + 智能制造”产业发展高峰论坛

亿赛通出席“互联网 + 智能制造”论坛

创新正在驱动消费互联网向产业互联网加速迈进。传统的制造业必须迎合时代发展，进行转型升级，即融合互联网、通信、大数据、云计算、人工智能等信息化和智能化手段进行深化改革和升级改进。对此，6 月 23 号，宁波市举办了“互联网 + 智能制造”产业发展高峰论坛。中国数据安全防护专家亿赛通，在十多年的数据安全行业发展中，长期携手制造业共同致力于数据安全管理工作。其数据安全防护的专业性、产品的前沿性、方案的独特性等促使亿赛通为中国企业转型和发展方式转变提供自己的一份力量。在本次重大论坛会议上，亿赛通精英伙伴与众多制造业参会嘉宾深入探讨“互联网 +、信息化以及智能制造”发展的新趋势，一起分享了亿赛通在各类企业和机构在智能制造领域的实践成果。

互联网下的转型升级 中国制造面临的安全威胁

在大会现场，亿赛通精英伙伴介绍到：制造设计行业随着信息化建设的推进，企业内部的数据流丰富了起来，制造业的信息安全投入比例虽然在不断加大，但投资策略主要集中在外部信息安全防护，如防病毒、防火墙、入侵检测等产品。而针对企业内部的核心数据信息安全防护，尤其是作为产品数据和管理数据这两大核心数据，无论是生产图纸、源代码、财务数据、经营分析还是交易信息等资料，对保密性都有着非常高的要求，这些因素都使行业信息安全需求强烈而又难以得到满足。因此，信息化时代下，内部不同的应用和管理的要求给设计制造业提出了很多新的要求。

智能防护 全新活力

亿赛通作为中国数据安全防护专家，通过多年的经验积累和不断的创新，成为实力雄厚、拥有完全自主知识产权的终端数据防护、应用数据防护、网络数据防护、存储数据防护、介质数据防护等智能化产品体系。公司针对制造设计行业的数据资产应用的特点，帮助企业核心数据资产安全管理系统解决了制造设计相关应用系统的数据安全防护要求，能够实现终端前台密文存储使用、服务器后台明文流转，消除文件从应用系统离线后的安全隐患。并且实现终端和应用系统数据的智能化安全管理。如亿赛通精英伙伴与参会人士分享了具体制造业经典案例，曾携手中国石油、中集集团、佳通轮胎、哈电集团、山鹰纸业集团等大型国家重量级制造企业实现了数据的智能化安全管理，从根本上解决了企业存在的信息泄密隐患，并通过高效、先进、智能化的数据安全技术手段，解决了企业数据的存储、使用和传输中可能存在的泄密问题；提供丰富的的审计记录，帮助员工提高安全意识。

当然，面对信息时代的爆炸式发展，亿赛通会不断创新、不断改进，永不止步的为企业制定完整的数据泄露防护解决方案，携手更多企业实现数据的智能化安全管控，以及实现企业核心信息资产防泄露的安全目标。

会议活动 | 亿赛通再次携手绿盟科技出席“智慧安全 2.0”南京站巡讲活动 共同构建智能安全

南京站：智网络 • 汇安全

6 月 23 号，由绿盟科技举办的“智网络 • 汇安全”绿盟科技智慧安全 2.0 全国巡讲活动南京站再次成功举办。亿赛通作为绿盟科技全资子公司，以及中国数据安全防护专家，携手绿盟再次出席南京巡讲会。在南京大会上，亿赛通与华东区域的所有与会嘉宾再次分享了智慧安全时代面临的挑战以及未来的发展趋势，并积极探讨了如何更好的满足华东市场的现实需求。

构建智能安全 走向智慧时代

在“互联网 +”的迅速发展背景下，新的发展趋势冲击着原有市场的发展状态，智慧安全已经成为当下发展不可逆转的方向。对此，“智能化”成为热议话题。在南京大会上，亿赛通精英伙伴以“智能诠释安全 --- 网络安全法实施后的企业数据安全思考”为主题，和与会嘉宾进行了深入的讨论。6 月 1 号，《网络安全法》正式实施，此法的出台从根本上填补了我国综合性网络信息安全基本大法、核心的网络信息安全法和专门法律的三大空白，并建立了全国统一的社会信用代码制度和信用信息共享平台，依法保护企业和个人的信息安全，从而走进了治理能力和治理体系现代化的总目标，走进了“智慧安全”的新天地。亿赛通数据安全防护解决方

案及产品迎接智慧时代 ,将智能安全产品融合数字化、网络化、智能化技术，以智能模块为单元满足使用中的数据、存储中的数据、传输中的数据、外带数据、离线办公数据、外发数据等各个环节的数据安全需求，让数据中心基础设施更加简单、高效、可靠。并对用户、应用程序和基础架构所生成的数据进行实时跟踪、监督，防护敏感数据外泄，有效的对客户敏感数据进行智能化综合防护管控。

专注安全 专业防护

通过亿赛通精英伙伴详细透彻的介绍下，现场嘉宾对其产品和方案产生了浓厚的兴趣。在智慧安全信息时代，亿赛通从未止步，在数据安全领域特别是数据安全产品和数据安全解决方案市场稳居市场前列，并在国内的智慧安全市场占据了一席之地。在核心技术上，坚持创新，拥有业内前沿的技术，带领行业前行。亿赛通数据安全防护产品及方案，坚持通过精心的顶层设计和完善的基础建设 ,并且从技术、服务、智能化管理手段等方面共同着手，推进“智慧安全”时代全面化进程做出努力。对于未来几年内数据安全市场的发展趋势、面临的挑战等一系列问题，亿赛通精英伙伴也深入的和不同行业的现场嘉宾进行讨论。亿赛通坚持与大家一路同行，坚持防护各大行业的数据资产 ,做好中国数据安全防护专家。

新一轮 Petya 病毒全球迅速蔓延
亿赛通 & 绿盟科技携手
跨越古都“西安”
共同扼杀新病毒 打造智慧安全 2.0

亿赛通 & 绿盟科技打造古都西安“智慧安全 2.0”

6 月 27 号，亿赛通携手绿盟科技跨进十三朝古都西安，成功举办了“智慧安全 2.0”巡讲活动。西安作为一个历史文化名城、世界四大古都之一，其城市经济、文化、政治都十分繁荣，备受国内外瞩目。对此，在互联网、云计算、人工智能等新的发展趋势下，促使西安的经济、政治、文化更加快速的发展，“智慧安全”成了城市发展的核心需要。那么，面对古都西安新的发展需求，在大会上亿赛通深刻的与古都参会嘉宾剖析了当下“智慧城市”发展状况，以及如何做好城市“智慧安全”，并进行了经典案例分享。

智慧城市 智能安全

亿赛通精英伙伴和西安古都嘉宾分析到当下智慧城市，是在新一代信息技术和知识经济的加速发展的背景下，以互联网、物联网、云计算等组合为基础，以信息技术高度集成、信息资源综合应用为主要特征，以智慧技术、智慧产业、智慧民生、智慧城市管理等为重要内容，实现城市各功能协调运作，为市民提供更高的生活品质。亿赛通作为中国数据安全防护专家，为全面建设城市高质量的生活方式和环境，提高人民生活的综合水平，积极配合各大城市努力建设“智慧城市”，打造“智慧安全”。如亿赛通伙伴分享到具体的成功案例，其公司智能数据安全加密产品，携手太原市、株洲市公安部对其网络安全进行智能化方案部署，对网络数据安全进行层层防护，实现对全网数据进行智能化的加密管控，有效的保护了其重要信息的安全，促进了太原市、株洲市公安部信息安全管理更加智能化、有序化，提高了智慧城市的建设能力。面对古都西安城市建设发展需求，亿赛通更加有信心携手打造“智慧安全”网络环境，实现西安市经济与社会的协调发展的智慧城市。

信息时代数据的繁荣 新一轮病毒措手不及迅速蔓延

数据已经成为一种新的经济资产类别，被誉为新世纪的石油和矿产。在互联网时代，面对各种网络攻击、窃取机密信息、以及数据资产的行为，如前段时间，全球近 100 个国家遭遇了勒索软件攻击，数万台计算机被感染。国内外各大企业、个人、团体单位行行业都开启应急措施，预防勒索病毒侵袭电脑数据。而且，近日，一个全新的名为“Petrwrap”的勒索软件正在全球肆虐，破坏了俄罗斯最大石油公司、乌克兰银行和一些跨国公司的电脑系统，以及英国、法国、德国、意大利、波兰和美国都有用户报告被感染，包括全球最大广告公司 WPP 、法国建筑材料公司 Saint Gobain，美国制药巨头默沙东 (65.54, -0.38, -0.58%) 等等企业。这种病毒一旦被感染，就会将每台电脑用私钥加密，使其无法使用，黑客要求用户向指定账户支付价值 300 美元的比特币，然后才给系统解密。

那么，面对这些突如其来的病毒攻击，亿赛通以在安全领域高度的专业性、专注性，和权威性，帮助各大企业预防病毒的突袭。通过自主研发的驱动数据防护核心技术，将数据实体与访问应用进行智能隔离和验证，屏蔽病毒软件读取终端上存储的数据，让病毒软件无论如何变种，都无法接触到用户数据，从而无法加密用户数据，使病毒攻击行为化为泡影。并且亿赛通还针对前段时间的勒索加密变成扩展名 .lock 的文件，可恢复被病毒加密的文件，而且已经成功帮助被病毒攻击的用户摆脱困扰。

在信息化飞速发展的时代，数据资产分分秒秒都可能面临着各种恶意病毒的威胁，要发展智慧城市，必须把城市的数据资产保护好，打造智能安全，才能促进现代化社会智慧城市的发展。亿赛通凭借优秀的智能数据安全产品、优质的服务、前瞻性的技术以及智能化的解决方案，和在数据安全领域的品牌地位，坚持推进智慧城市建设，坚持对抗各种恶意病毒攻击数据的行为，为城市信息资源共享、城市运转高效、公共服务便捷的智慧之城努力奉献出自己的力量，让智能安全在中国的每一个角落打响嘹亮的号角，为智慧城市建立提供强有力的“智力”支撑。

《网络安全法》6 月 1 日正式实施 7 章 79 条内容 5 大亮点与你我息息相关

《网络安全法》从 2015 年 6 月初审，经历 3 次审议，到 2016 年 11 月 7 日正式出台。昨日（6 月 1 日）《中华人民共和国网络安全法》、《互联网新闻信息服务管理规定》、《网络产品和服务安全审查办法（试行）》等一批互联网领域的法律法规正式施行。《网络安全法》的颁布实施，对于保障网络安全、维护网络空间主权和国家安全、社会公共利益、保护公民、法人和其他组织的合法权益具有十分重要的意义。亿赛通从事数据安全防护领域十四年，已发展成为国内数据安全、网络安全及安全服务三大业务供应商，以上百项知识产权涵盖了包括：终端、网络、存储、审计等多个方面的几十个数据安全软硬件产品，坚持为广大客户提供核心技术保障。对此，从专业、专注的态度，为您详细剖析与你我息息相关的法律相关内容。

《网络安全法》与网名息息相关的权利与义务

相关义务

1、任何个人和组织不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布与实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动有关的信息。

2、网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

3、网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务时，用户不提供真实身份信息的，应当拒绝提供相关服务。

4、网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户，并向有关主管部门报告。

相关权利

1、个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。

2、从事网络安全相关行业的企业可以考虑申报国家项目资助，可以提升企业服务水平，便于承接政府和企业购买的社会化服务。

3、各类院校也可以积极申报网络安全人才培养专业，申请相关的课题，加入到国家网络安全促进的战略里面来。可以预计，网络安全产业将会迎来大发展，机遇不断。

《网络安全法》正式实施 五大亮点值得关注

本次颁布施行的《网络安全法》共七章七十九条，主要包括：维护网络主权与合法权益、支持与促进网络安全、强调网络运行安全、保障网络信息安全、监测预警与应急处置、完善监督管理体制、明确相关利益者法律责任等七大方面，五大亮点如下：

亮点 1：明确对公民个人信息安全进行保护

网络安全法第四十四条规定：任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

亮点 2：个人信息被冒用有权要求网络运营者删除

网络安全法第四十三条规定：个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息。网络运营者应当采取措施予以删除或者更正。

亮点 3：个人和组织有权对危害网络安全的行为进行举报

网络安全法第十四条规定：任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

亮点 4：网络运营者应当加强对其用户发布的信息的管理

网络安全法第四十七条规定：网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

亮点 5：未成年人上网有哪些特殊保护？

网络安全法第十三条规定：国家支持研发开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

对于《网络安全法》的正式实施，亿赛通强力支持国家政策，并且努力从技术方面持续为大家的数据安全保驾护航，携手国家政策共同致力于建设安全、高效、文明、和谐的网络安全环境。

U 盘“替身”病毒正在全国范围内大量交叉感染 毕业季论文是关键呼叫大神有招吗？

刚刚过去的 WannaCry 让人们见识了勒索软件的厉害。然而近日，一款名为“替身”的 U 盘病毒正在全国范围内大量交叉感染，各地打印店的电脑成为病毒传染扩散的载体。时值毕业季，中国数据安全防护专家亿赛通着实为各位即将毕业走入工作岗位的大学生感到焦虑，因为学生群体打印毕业论文等资料时极易遭到此类病毒攻击。

“替身”病毒究竟是何方妖孽？

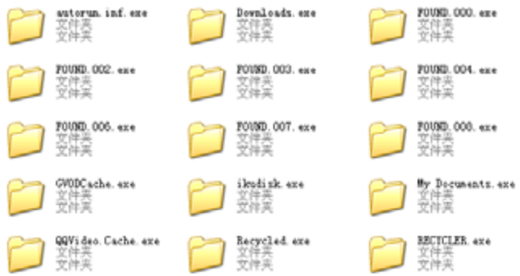
据介绍“替身”病毒具有很强的迷惑性，会把 U 盘里的文件资料隐藏起来，并创建与被隐藏资料相同名称的快捷方式作为“替身”。如果受害者在使用电脑时双击打开快捷方式，U 盘里的病毒就会被激活运行，感染它所连接的电脑，从而实现在不同电脑间快速交叉传播。与以往常见的 U 盘病毒不同的是，“替身”病毒更顽固，它会启动一个“守护”进程专门保护病毒。

通常情况下，我们普通的 U 盘没有进行加密保护的状况下，就会容易被病毒入侵、敏感资料被窃取、非法用户易识别等状况，而加密后的 U 盘可以将 U 盘存储的重要资料进行保护，即使病毒入侵，非法用户也无法获得敏感数据。

小贴士：U 盘安全防护计谋

计谋一：不能手动删除快捷方式，这样会导致 U 盘资料被病毒清空；

计谋二：如果发现病毒感染情况，先紧急使用专业安全的查杀软件对 U 盘进行杀毒；



计谋三：要想彻底预防类似 U 盘病毒交叉感染事件发生，要从根源去彻底预防病毒。亿赛通全盘加密安全 U 盘为亿赛通自主研发，是国内较专业的基于物理磁盘全盘加密技术（FDE）的安全 U 盘。它通过硬件控制方式对 U 盘存储区域进行保护，双因子认证技术确认访问权限，杜绝暴力破解或底层非法入侵，彻底防止了非法用户窃取敏感资料，从而保护用户 U 盘核心数据安全和打印安全。

亿赛通全盘加密安全 U 盘在产品研发设计过程中，严格根据国家关于存储介质管理的技术要求，结合知名安全硬件厂商提供的芯片技术，对 U 盘实体进行全盘加密保护真正做到：

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、病毒入侵等都无法获得 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 盘具备日志审计智能化的功能，对操作行为可记录和追踪。

高考之后招生诈骗案件进入了活跃期
如何识破这些“诈骗”手段？

一年一度紧张的高考终于结束，十年磨一剑，相信 2017 届的莘莘学子通过历练，一定会走向自己心目中的诗和远方。高考虽已结束，但是很多家长和考生仍然没有放松警惕，因为高考，是大学招生的手段；高考，是十二年寒暑交替苦读的学子进入大学深造的独木桥；高考，是个人人生的分水岭。今天，虽然读书不是唯一的出路，但是：提干要文凭，升职要文凭，进入国家机关工作要文凭，登大雅之堂要文凭，评论一个人的品味和素质也是看文凭……

根据往年经验，每年高考之后，形形色色的招生诈骗案件进入了活跃期，家长心中的急切、侥幸甚至是上当受骗后碍于面子不愿声张的心态，都成了骗子们手中的小尾巴。中国数据安全防护专家亿赛通教您如何识破“诈骗手段”。

小贴士防护专家：“诈骗”手段防范注意事项

1、“特殊招生类型”诈骗

不法分子利用“自主招生”、“定向招生”、“委培生”等政策，称可以降分录取，甚至不用高考成绩自主选拔学生，骗取几万甚至几十万元钱财。

亿赛通小贴士提示：入选考生高考成绩须达到所在省、区、市确定的与试点高校同批次录取控制分数线。自主招生不是“自由招生”，没有提前报名，入选更不可能通过自主招生录取。

2、“高考志愿填报”APP 内置手机病毒

不法分子向考生和家长发送带有木马病毒链接的短信，或是在网站上设置一个诱骗性的木马链接，只要点进去，木马程序便植入手机，获取关联银行卡等信息，拦截支付验证码，转账提现。

亿赛通小贴士提示：不要在手机论坛、非安全电子市场下载此类手机应用，并定期查杀病毒。

3、伪造虚假查分网址

诈骗分子通过窃取考生个人信息，然后诈骗短信发送虚假查分网址，让考生输入个人信息及银行账号后将这些信息记录并贩卖，或者根据这些信息进行精准电信诈骗。

亿赛通小贴士提示：查分认准当地教育主管部门指定的查分网址，同时谨防各类涉及查分、录取的相关短信。

4、提前获知录取结果

在录取信息正式公布前，以可提前获取录取信息为名，骗取考生及家长钱财。

亿赛通小贴士提示：考生及家长应以本地教育部门官方网站或者报考院校的官网公布的录取信息为准，切勿听信提前获取的谣言。

5、寄送伪造的录取通知书

嫌疑人在窃取了学生个人隐私信息之后，通过邮局向考生寄送伪造的录取通知书，加盖“公章”和“录取编号”，骗取考生和家长的信任，让考生将学杂费打入银行账号内。由于伪造的录取通知书仿造正品印制，且印有招生办录取专用章，考生收到通知书后，如不仔细查看，很可能上当受骗。

亿赛通小贴士提示：按照教育部规定，普通高校录取通知书由招生学校根据省、市级招办审核备案的录取名册发放，并加盖省、市级招办录取专用章。考生拿到通知书后，可登录省、市级招生考试信息网或到区（县）招生办查询自己的录取信息。

6、接到各种诈骗电话

高考之后，很多诈骗打电话打着学校资助的幌子要求学生给银行卡打钱、或者提前交学费等情况，基本都是诈骗电话。如去年徐玉玉一案事发后，引起舆论热议。教育部高度重视，并且教育部官网就此专门发布通报，提醒准大学生谨防诈骗，“无论是哪个单位或者个人提供资助，不应要求学生到 ATM 机或网上进行双向互动操作。

亿赛通温馨提示：如有类似要求的，请先向老师和当地教育部门咨询，千万不要擅自按照对方要求操作转账，以免上当受骗。

亿赛通温馨祝福

互联网高速发展的今天，各种诈骗手段防不胜防，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、招生处、学校等相关单位也必须高度重视，注意保护好学生个人信息，不要被诈骗分子窃取敏感信息，从而让其实施诈骗行为，对学生造成很大伤害。我们知道《网络安全法》于本月 6 月 1 日起正式实施，标志着我国维护网络与信息安全的工作进入一个全新阶段，作为首部统领国家网络安全工作的综合性法律，以维护国家网络空间主权、安全和发展利益为根本，以筑牢网络安全防线为目标，为网络强国建设大业保驾护航。那么，亿赛通作为专业的数据安全防护专家，肩负起信息安全保护的责任，全力支持各学校及相关单位共同倡导大家加强防护意识，保护好学生信息，大家务必引起重视，千万不能在让徐玉玉类似悲惨事件再次发生。

最后，亿赛通衷心祝愿所有莘莘学子都能够顺利考入自己理想的大学，赶赴下一段人生旅程。

不要比特币 亿赛通帮您恢复被勒索加密的数据资产

各种数据被勒索软件加密，

肿木办？宝宝真心急啊，

急！急！急！

大神，求解啊！

勒索软件加密类型多样，

但被勒索加密变成扩展名 .lock 文件的，

亿赛通有解密答案，

亿赛通有解密答案，

亿赛通可恢复被勒索病毒加密的 .lock 文件，

已经成功帮多家用户摆脱困扰，

让文件正常打开，读取原数据。

从被勒索加密到成功解密过程如下图：

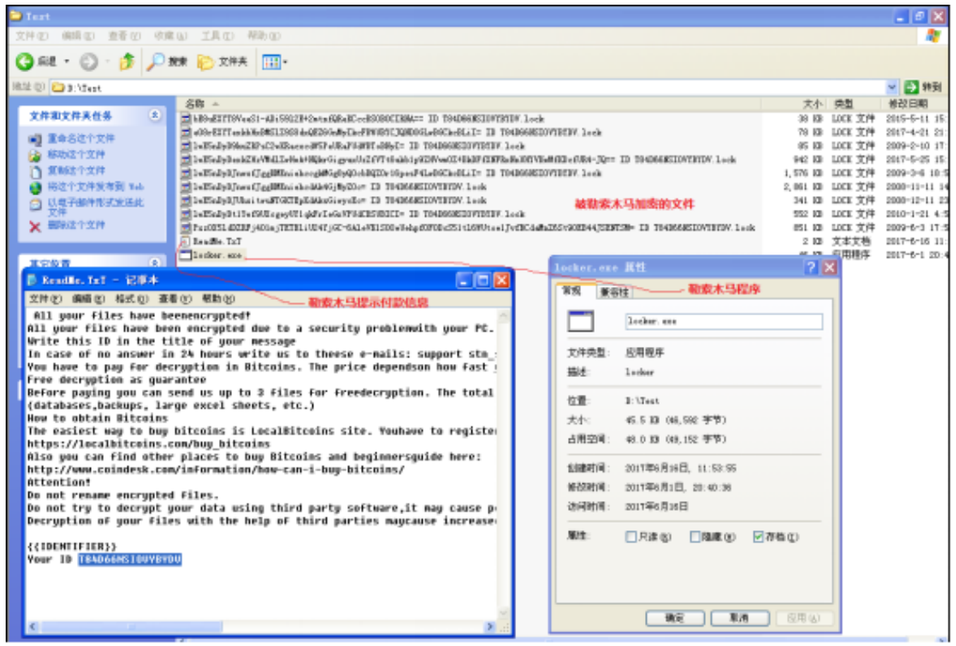


图 1：被勒索木马加密的文件

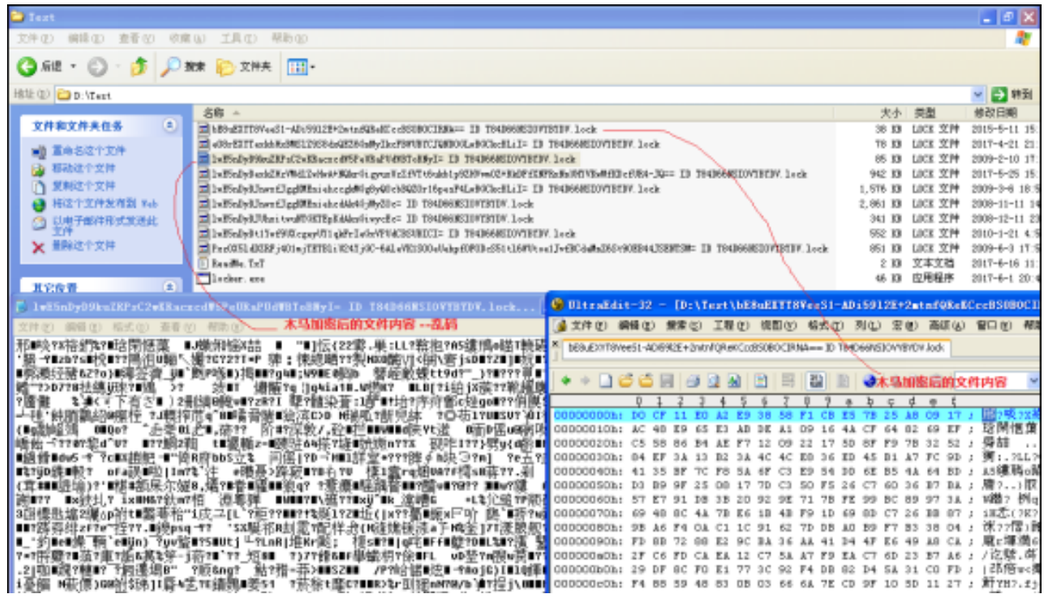


图 2：木马加密后的文件——乱码，无法打开

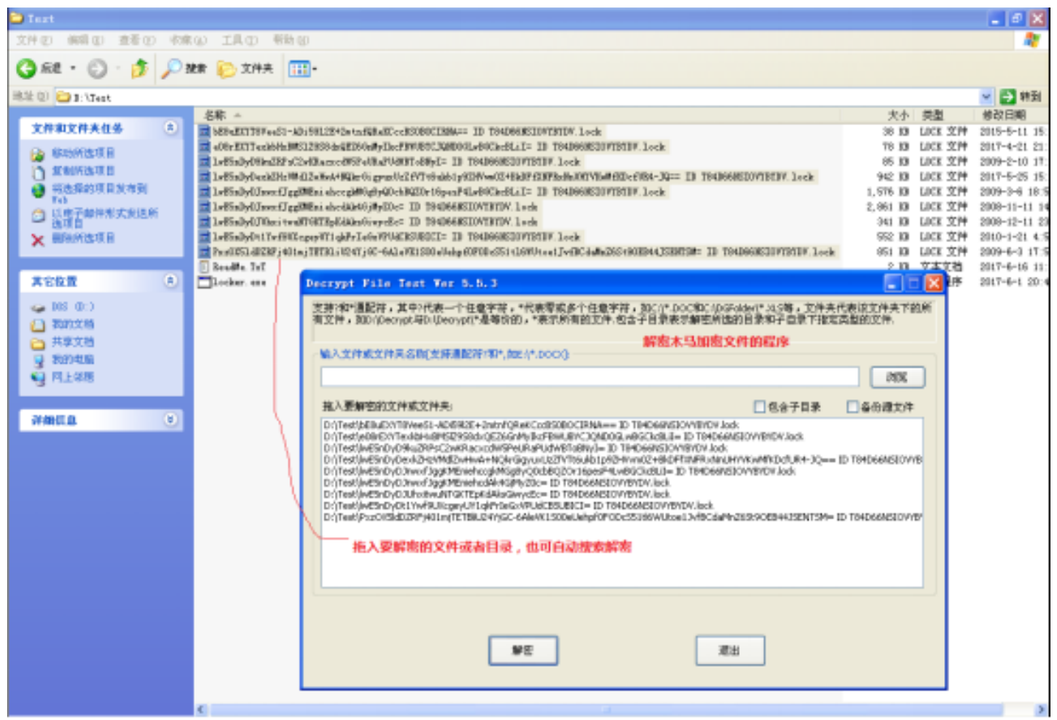


图 3：解密木马加密文件的程序——开始解密

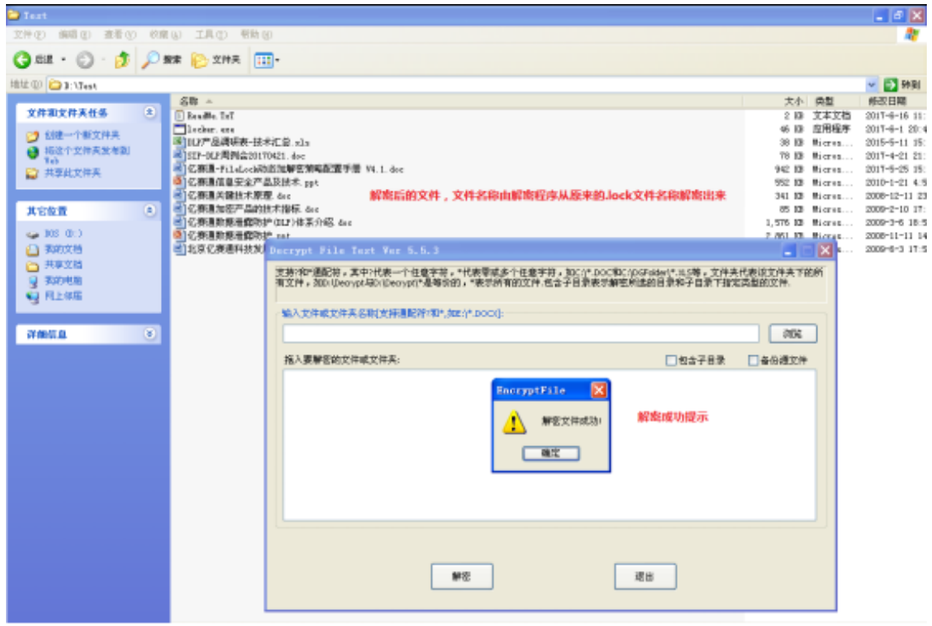


图 4：解密后的文件，文件名称由解密程序从原来的 .lock 的文件名称解密出来

图 5：解密后的文件内容——解密成功

所以，

还有被勒索加密耍流氓急哭的宝宝们，

赶紧联系亿赛通，

无需在本机操作，

只要您把被勒索加密的文件交给我们即可。

勒索软件变种很多，

我们也是根据手中的样本搞定了一类，

也欢迎小伙伴把其他样本和我们一起研究，

一同抵制打击非法勒索黑产。

亿赛通不仅帮您解密，还能帮您防御勒索软件！

设计 / 制造业深度融合互联网新发展模式 亿赛通协同推进“中国制造 2025”保障数据安全

行业分析

随着制造业信息化的迅速发展，企业信息，尤其是文档信息如何能更有效、更安全的流转和使用成为生产商所关心的问题，文档信息的安全传输也随之成为一项重要的业务需求。制造业是我国国民经济的重要支柱产业。大部分企业，尤其是制造型企业，随着信息化建设的推进，在网络方面增加了硬件设备，在软件方面，增加了 ERP、PDM、CRM 和 SCM 等专业系统，企业内部的数据流越来越丰富。伴随着愈来愈激烈的行业竞争，数据安全问题就显得尤为重要。

据权威机构调查，80% 以上的安全威胁来自泄密和内部人员犯罪，而非病毒和外来黑客引起。防火墙、入侵检测、隔离装置等网络安全保护对于防止外部入侵有着不可替代的作用，而对于内部泄密显得无可奈何，真正有目的盗取或破坏信息的黑客也许正在隐藏在内部。企业内部的信息安全需要一个整体的策略方案，以巩固信息化成果，降低企业信息安全风险。

需求背景

在制造、设计高度信息化、网络化的趋势带动下，企业引入了大量与生产制造相关的应用系统，而这些应用系统在存储、使用、传输、交互的过程中都会造成数据泄密。具体表现如下：

1. 系统内产生的数据和文档有高度保密性、高度敏感性，数据泄露会造成重大危险；

2. 企业的认证体系、业务信息系统和办公 OA 系统等应用平台数据交互频繁 ,与合作单位有大量的对外接口；

3. 企业内部网络有多种业务平台，移动设备如笔记本电脑、U 盘使用广泛；

4. 与外部单位的合作，对外发出文件数量较多；

5. 办公网上的信息都未被加密，采用明文传输；

6. 办公网的用户权限控制不严密。

解决方案

亿赛通数据泄露防护（DLP）是专为企业级用户设计的数据防泄密解决方案，从数据的存储、传输、交换过程中的安全环节，采用了多种加密手段结合的方式保护。从终端、网络和存储三个层次入手，对核心数据的形成、存储、使用、传输、归档及销毁等全生命周期进行安全控制，结合企业特有的业务需求、业务模式和管理文化，为企业制定完整的数据泄漏防护解决方案，实现企业核心信息资产防泄漏的安全目标。

1. 加密系统：采用亿赛通数据泄露防护系统（DLP），运用透明加密、主动加密和智能加密的梯度式加密方式，对设计图纸、文档、财务报表、业务合同等核心数据进行保护。从数据的产生，到数据使用传输，数据都处于加密状态，从源头保证数据的安全；

2. 采用亿赛通安全准入网关，通过 DLP 系统加准入网关的方式对 OA、MES、SVN 业务系统的安全保护及终端电脑文件的自动加密保护，达到数据安全从源头做起，凡事从业务系统下载下来的数据都已经做过加密处理，员工拿到的数据就已经是加密文件，但服务器中保存的文件仍保持明文状态；

3. 采用亿赛通数据泄露防护系统（DLP），对内网使用的多种系统进行统一平台管控。对终端、网络、邮件、移动终端、端口等进行多层次防护，保护文档安全；

4. 采用亿赛通数据泄露防护系统的外发管理，可以将外发文档进行统一管理，通过设置外发信息的秘钥、权限、机器码绑定等设置，文档是无法打开的，保证了与外部单位合作的外发文档的安全。

方案价值

亿赛通数据泄露防护系统（DLP）解决方案与企业的安全理念、安全需求高度融合，从根本上解决了企业存在的信息泄密隐患；通过高效先进的数据安全技术手段，解决了企业数据的存储、使用和传输中可能存在的泄密问题；提供丰富的的审计记录，帮助员工提高安全意识。

亿赛通 DLP 提升中集集团等级管理建设能力 助力企业实现智能化数据安全防护体系

中集集团简介

中国国际海运集装箱（集团）股份有限公司（简称“中集集团”），是世界领先的物流装备和能源装备供应商，总部位于中国深圳。公司致力于集装箱、道路运输车辆、能源和化工装备、海洋工程、物流服务、空港设备等，提供高品质与可信赖的装备和服务。其市场占有率而言，中集有 10 多个产品持续多年保持全球第一，作为一家为全球市场服务的跨国经营集团，中集在亚洲、北美、欧洲、澳洲等地区拥有 200 余家成员企业，客户和销售网络分布在全球 100 多个国家和地区。

需求背景

《网络安全法》第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。那么，中集集团作为世界优秀的物流装备供应商，企业的信息安全至关重要。随着中集集团业务快速扩展，集团经营规划、行政办公、技术研发资料愈发重要，集团需要统一梳理核心数据并明确各级数据保护规范和要求。集团下属 50+ 分公司，研发资料、项目文档技术保护手段和管理存在缺失，资料外泄情形屡有发生，核心重要资料容易被竞争对手窥视，许多重要资料随着人员离职等大量流失。集团出现部分数据泄密事件后审计无从做起，相关职责划分不明确，缺乏技术手段。

解决方案

亿赛通数据泄露防护（DLP）系统是一款基于内容识别技术的保护系统。

终端防护：防止敏感数据通过打印、刻录、聊天工具、发送邮件等终端方式泄露出去。

网络防护：防止敏感数据通过邮件、网盘、微博、FTP、论坛等网络方式泄露出去。

数据扫描：通过扫描和分类的方式，随时随地发现企业敏感数据分布，并保护静态数据。

邮件防护：防止敏感数据未经任何检查通过企业邮箱泄露出去。

数据分析：基于规则和中文语义的智能数据分析，对数据进行高效敏感检查。

审计报表：提供统计分析能力，实现安全现状可度量、事件可追溯、态势可查询。

项目成果

亿赛通完善的数据泄露防护（DLP）解决方案，为中集集团建立了一套数据资源保护标准，防止员工的不安全行为引入风险，以及保障了各个环节数据的安全运行，并且使得员工了解与自己相关的数据安全保护责任，强调数据系统安全对企业业务目标的实现、以及业务活动持续运营的重要性。

亿赛通智能感知中国石油敏感数据助力公司实现内网综合一体化防护

客户简介

中国石油工程建设公司（英文缩写 CPECC）隶属于中国石油天然气集团公司，是集团公司专门从事石油工程设计、制造、施工和工程总承包的专业公司，现已发展成为集团公司在国内外石油工程建设领域最具代表性的公司。CPECC 历史悠久，建设功能完善，技术力量雄厚，拥有一大批熟悉国际惯例、技术水平高、管理经验丰富的专业技术和管理人才，具备设计、采购、制造、施工一体化全功能。自 2003 年以来，先后获国家、省部级以上优秀工程勘察设计奖 48 项，优质工程奖 28 项；荣获全国对外承包“十佳”企业、“AAA 级信用企业”、“全国百强设计院”、“全国 100 家最佳建筑企业”等荣誉称号。

典型案例 TYPICAL CASES

需求背景

中国石油工程建设公司作为国家重要的涉密单位，在整体信息化安全建设方面先后已经针对物理安全、网络安全、系统安全等做了相关建设并已经取得很好成效，但是在数据安全层面中国石油工程建设公司没有通过技术手段去保护数据的安全，数据安全存在一定风险漏洞。对此，公司结合当下的信息安全现状，最终决策采用亿赛通文档安全管理系统保护企业的数据安全。

解决方案

智能透明加密：实现对任意文档自动透明加密的同时，不影响用户的使用习惯；

内容安全防护：防止核心数据通过复制拖拽、截屏录制、打印输出以及副本另存等方式泄密；

安全水印支持：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所带来的泄密风险；

身份认证集成：支持与基于 Ldap 和 OpenLdap 协议的统一身份认证平台（如 AD、ED、TDS 等）进行无缝集成，如实现组织架构及用户账号信息的自动完整同步和单点登录认证集成等；

离线办公支持：可通过离线审核、策略预设及离线补时等功能满足各种离线办公要求；

开放式策略库：用户可根据业务及管理需要进行安全策略自定义，开放、灵活的策略配置可降低企业后续维护成本；

细粒权限控制：细化设置文档的阅读、编辑、复制、打印等组合权限，并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、归档、交接管理及版本变更管理等功能。

项目成果

亿赛通文档安全管理系统的部署使得中石油工程建设公司内部文件可以在所有涉密终端上无障碍流转，如需将文件发送到第三方公司必须由本部门文档管理员解密，并且对于每天大批量的图纸需要委托给第三方专业打印公司生成纸质图纸，在发送前将电子文件转化成外发加密文件，从而保障图纸不会被第三方打印公司泄密，确保了中国石油工程建设公司所有数据实现智能化的管理有序，并安全运行。