

比特专访 | 亿赛通：书写数据安全领域新版图

CNNVD 公布 WannaCry 勒索软件攻击事件分析报告



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

網址：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

4-6 CNNVD 公布 WannaCry 勒索软件攻击事件分析报告

7-9 十五大统计数据描绘网络安全行业市场蓝图

10/11 大数据产业的 " 生力军 "

12/13 快递行业举行首个信息安全峰会 " 隐私面单 " 让个人信息不再 " 裸奔 "

亿赛通动态 ESAFENET NEWS

14/15 媒体专访 | 绿盟科技 2016 年报综述：亿赛通顺利完成业绩承诺

16/17 活动会议 | 亿赛通出席 2017 年湖北省勘察设计协会交流会 建立可持续发展信息安全管理体

18/19 比特专访 | 亿赛通：书写数据安全领域新版图

20/21 智网络 • 汇安全 亿赛通携手绿盟科技出席 " 智慧安全 2.0 " 全国巡讲活动

22/23 《网络安全法》如火如荼 亿赛通参加 2017 珠海 " 互联网 + 时代的信息安全 " 论坛活动

亿赛通小贴士 ESAFENET PROMPT

24/25 与其亡羊补牢 不如阻断根源

26/27 老干妈重大商业机密遭窃取？泄密真相引发各大 BOSS 深思 溺宠的企业骨干是否割爱留一招？

28/29 《网络安全法》6 月 1 日起即刻实施 这些 " 安全 " 知识 You 必须 get 到！

典型案例 TYPICAL CASES

30/31 防范和化解敏感信息泄密风险 亿赛通携手长城证券建立信息防泄露体系

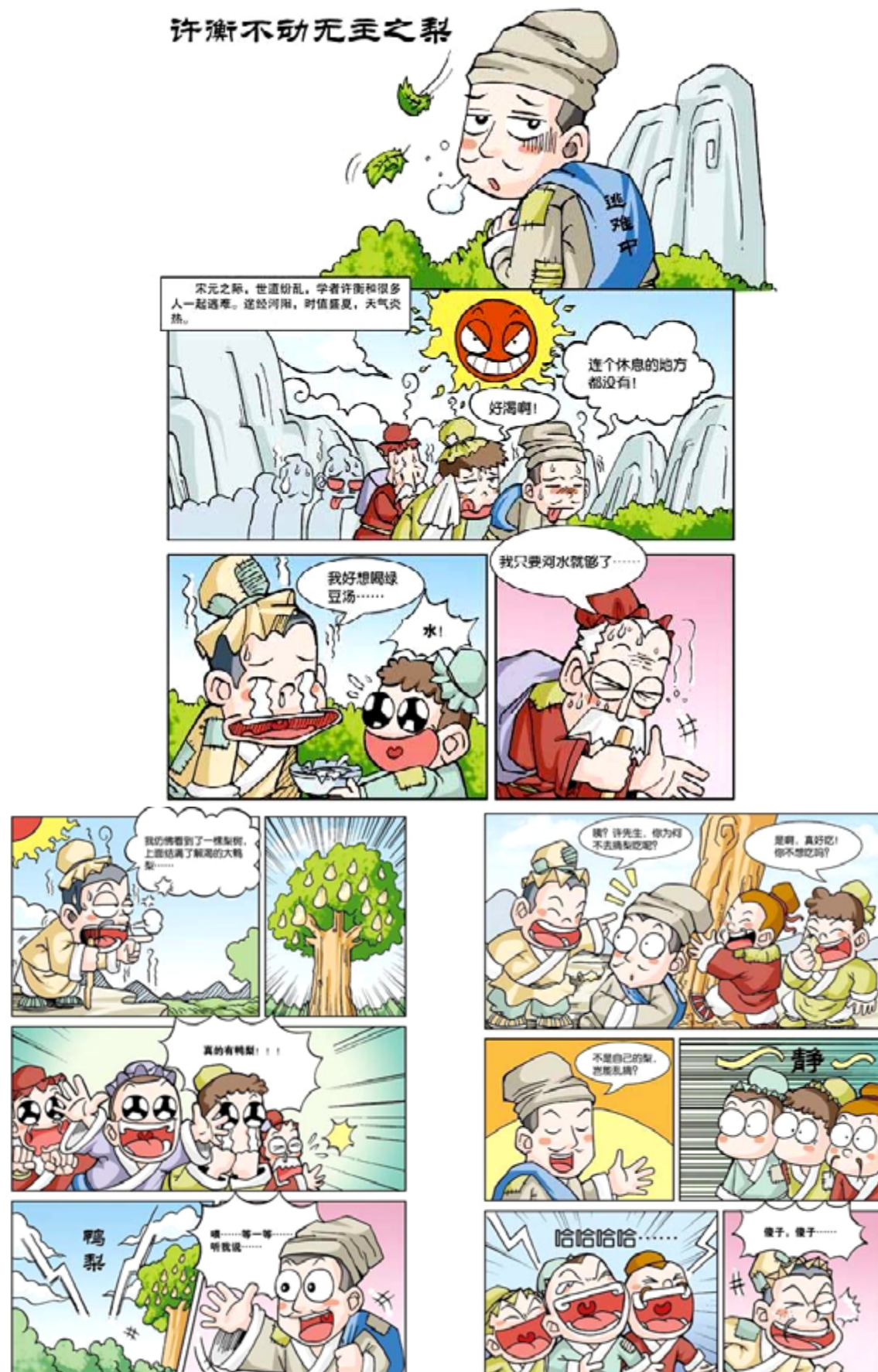
32/33 浦发银行签约亿赛通有效制定安全策略 共铸 " 数据安全 " 坚强堡垒

34/35 中国建设银行携手亿赛通部署最优数据安全解决方案 保障银行数据无懈可击

员工天地 STAFF CORNER

36/37 粽情端午 --- 亿赛通送祝福

许衡不动无主之梨



“梨虽无主，我心有主”

有这样一个故事，说的是元代大学者许衡一日外出，因天气炎热，口渴难忍。路边正好有一棵梨树，行人纷纷去摘梨，惟独许衡不为所动。有人便问：“何不摘梨以解渴？”他回答：“不是自己的梨，岂能乱摘？”那人笑其迂腐：“世道这样乱，管他谁的梨。”许衡正色道：“梨虽无主，我心有主。”……

“梨虽无主，我心有主”，意味着一个人能够坚持信念，恪守自己的操行，这是一种准则、一种修养、一种境界、一种精神。那么，放到企业更应如此，亿赛通从创立之初到如今，14年坚持打造数据安全行业，以专业、专注的态度，秉承“服务客户、持续创新、勇担责任，专业至上”的核心价值观，努力做好数据安全行业，不断创造行业传奇。

数据就像农业社会的土地、工业社会的能源一样，成为信息社会最重要的生产要素和资源。为此，亿赛通五月刊再次新鲜出炉，而又恰逢端午，应是良辰，纵览本月数据安全行业发展最新动态。移动互联网、智能终端、云安全、大数据等快速渗透到地球的每一个角落，联网设备产生的数据量呈几何级数增长……面对新的信息安全挑战和机遇，数据安全企业如何应对？未来，如何继续开辟新道路？本期月刊犀利为您解读，全新书写数据安全领域新版图……

CNNVD 公布 WannaCry 勒索软件攻击事件分析报告



北京时间 2017 年 5 月 12 日，一款名为“WannaCry”（也称 WannaCrpt、WannaCrpt0r、Wcrypt、WCRY）的勒索软件在全球范围内爆发，造成极大影响。针对本次攻击事件，国家信息安全漏洞库（CNNVD）进行了分析研究，情况如下：

一、网络攻击事件背景

此次爆发的“WannaCry”勒索软件主要借鉴了针对微软 Windows 系统漏洞的利用工具“永恒之蓝”（EternalBlue）进行传播扩散。2017 年 4 月 14 日，黑客组织 Shadow Brokers（影子经纪人）公布了黑客组

织 Equation Group（方程式组织）的部分泄露文件，文件涉及多个 Windows 操作系漏洞的远程命令执行工具，其中即包括“WannaCry”勒索软件攻击事件中所涉及的“永恒之蓝”利用工具。“WannaCry”勒索软件借助“永恒之蓝”漏洞利用工具，利用 Windows 操作

系统在 445 端口的安全漏洞（CNNVD-201703-721 ~ CNNVD-201703-726），潜入电脑对多种文件类型加密，并弹出勒索框，向用户索要赎金（以比特币支付）用于解密。

二、“WannaCry”勒索软件技术特点及危害

（一）攻击特性

爆发突然。短短一天内，在几乎毫无任何预兆的情况下，百余个国家和地区遭受攻击并呈现蔓延态势。行为恶劣。勒索蠕虫一旦成功入侵，将加密系统内全部文档，并通过破坏硬盘快照的方式增加系统恢复难度，不交付赎金（单机解密赎金 300 美元至 600 美元，一般通过比特币支付）无法解密。自动传播。可利用 Windows 平台所有版本（winXP、Vista、Win7、Win8、Win2003、Win2008、Win10 等）的漏洞进行自动传播，未打补丁的机器极易感染并在内外网快速传播。难以解密。勒索软件使用 AES128 加密文件，使用 RSA2048 公钥加密 AES 密钥。就目前情况看，基本无法通过计算或碰撞的方式进行解密，国内有企业提出通过设法恢复被删原文件方式找回原始未加密文件。通信匿名。勒索软件进行攻击后，会自动释放 Tor 网络组件，用于解密程序的网络通信，赎金使用比特币支付，使勒索过程难以追踪溯源。时间掐准。此次攻击发生正值周末，据分析在我国爆发时间应为周五下午 3 点左右，恰逢国内周末时间。攻击意外中断。勒索软件中预留了终止机制，即访问一个超长域名成功时，攻击传播就会停止。美国洛杉矶威胁情报公司一名员工注册了该域名开启了停止机制，域名启用后每秒访问 IP 过千。

（二）现实危害

文档损失。遭受攻击的各类文档均被加密，无法访问使用。系统停服。系统会不断弹出交付赎金的窗口，无法正常使用。解密存疑。目前尚无对交付赎金进行解密操作的分析，不确定是否能够正常解密。

（三）潜在风险

内网蔓延。尚未出现爆发大规模感染的情况，但分析其代码可知，内网蔓延的隐患仍然存在。变种变异。随着杀毒软件和安全防护措施的升级，“WannaCry”勒索软件若想避免查杀继续存活，或会改变特征值，而为继续感染更多计算机，也可能利用新的漏洞进行换代升级。

三、全球遭受网络攻击总体情况

（一）网络攻击涉及的范围广

此次网络攻击涉及百余个国家和地区的政府、电力、电信、医疗机构等重要信息系统及个人电脑遭受严重网络攻击，最严重区域集中在美国、欧洲、澳洲等。截至目前，全球攻击案例超过 75000 个。

（二）网络攻击无明显地域 / 行业分布特点

从受攻击目标类型与地域分布来看，此次攻击未表现出显著的地域与行业分布特点，与“WannaCry”随机扫描传播机制一致，攻击无明显指向性和目标性。

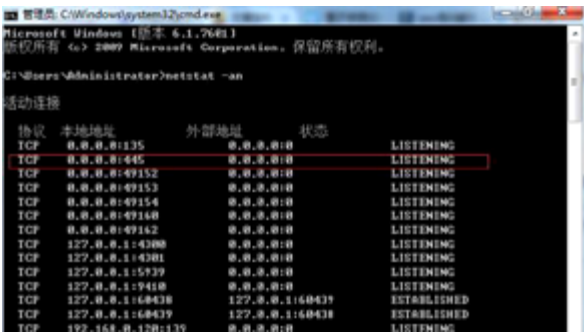
（三）各方积极应对与防范

各国政府谨慎应对。尚无国家政府宣称已经调查掌握事件幕后详细情况。英、德、俄、美等多个国家向本国公民及机构发出警告，要求尽快更新补丁，做好计算机数据备份等防护工作。对于已感染设备中被加密的文件，目前各国政府及信息安全企业均无法提供有效的数据破解恢复手段。英国政府国家网络安全中心（NCSC）称其第一时间启动了针对事件及攻击者的调查；德国、俄罗斯政府网络安全机构也作出了类似表态。相关安全企业开展技术分析。

研判分析认为，目前较为明确的攻击幕后背景线索主要是从代码中逆向分析发现的三个比特币钱包地址以及五个暗网命令控制服务器，各国网络安全与司法调查机构均已锁定了这些目标，通过各方合作，力求尽快发现攻击者的实际背景情况。

十五大统计数据描绘 网络安全行业市场蓝图

在技术领域，网络安全目前是发展最快的一大产业。为把握该市场脉搏，美国网络安全公司 CybersecurityVentures 列出了 2017 年网络安全行业的 15 大统计数据。



四、处置建议

“WannaCry”勒索蠕虫是勒索软件类病毒中全球首例使用远程高危漏洞进行自我传播的蠕虫，加密编程规范，如不公开私钥，很难通过其他手段对被加密勒索的文件进行解密，为此建议：

（一）应急措施

1、立即断网，防止扩散和蔓延。对于已经感染“WannaCry”勒索蠕虫的计算机，尽快关机，取出硬盘，通过专业数据恢复软件进行恢复。立即切断内外网连接，避免感染网络中的其他计算机。

2、启动恢复程序，及时修复补丁。若计算机存在备份，应启动备份恢复程序，及时安装修复补丁。

（二）防范方案

1、个人用户采取应急措施，安装漏洞修复补丁。“WannaCry”勒索蠕虫利用的是微软官方的 SMB 漏洞，

请个人用户及时检查安装 MS17-010 修复补丁。与此同时，及时采取临时解决方案，一是关闭计算机的 445 端口，二是配置主机级 ACL 策略封堵 445 端口，三是打开“Windows 防火墙”，进入“高级设置”，在入站规则中禁用“文件和打印机共享”相关规则。

2、网络管理员修改网络配置，监控网络接口。建议各网络管理员在网络防火墙上配置相关策略，限制外部对 445 端口的访问，加强内网审计。同时在接入交换机或核心交换机抓包，查看是否存在大量扫描内网 139、135、445 端口的网络行为，及时定位扫描发起点，对扫描设备进行病毒查杀，一旦发现被感染主机，立即断网防止进一步扩散。

（三）日常使用规范

在日常计算机使用过程中，对重要信息数据定期及时进行备份；浏览网页和使用电子邮件的过程中，切勿随意点击可以链接地址；及时更新操作系统及相关软件版本，实时安装公开发布的漏洞修复补丁。（新闻来源：IT 之家）

1. 消费

未来 5 年，全球网络安全消费预测累计超 1 万亿美元。2004 年，全球网络安全市场价值仅 35 亿美元，2017 即将增至 1200 亿美元。网络安全市场在 13 年间增长了约 35 倍。



2. 网络犯罪

到 2021 年，全球网络犯罪造成的损失预计将达 6 万亿美元，2015 年这个数字是 3 万亿美元。这里所指的损失，包括了数据损坏、资金被盗、生产力损害、知识产权被窃、个人和金融数据被盗、侵吞公款、诈骗、正常业务过程遭攻击中断、取证调查、数据和系统恢复，以及信誉伤害。



3. 岗位

2017 年网络安全岗位空缺有 100 万个，预计到 2019 年这一数字将增至 150 万以上。人才短缺的情况为更丰富多彩的劳动力组成创造了机会，女性和少数族裔将有机会进入该万亿美元领域。



4. 失业率

2017 年，网络安全失业率维持在 0%(与 2016 年相同)。PaloAlto 研究中心报告称，2019 年，全球网络安全人才需求将达 600 万。这意味着，失业率指针在短期内都不会有任何挪动。



5. 培训

到 2027 年，安全意识培训市场预计将达 100 亿美元 / 年。培训员工识别和防御网络攻击，是网络安全产业中投入最不足的行业。



6. 医疗保健

2017 到 2021 的 5 年间，全球医疗保健行业网络安全花费预测累计将超 650 亿美元。随着医疗保健行业继续推进各项信息的数字化，网络罪犯的目光也越来越投注于该行业。未来 10 年医疗保健安全市场的增长会有许多推动因素，该动态位列其一。



7. 勒索软件

到 2020 年，对医疗保健机构的勒索软件攻击预测将有 4 倍的增幅。詹姆斯·科米，刚刚被免职的前 FBI 局长，最近在波士顿网络安全大会 (BCCS2017) 上发表了主题演讲。当被问到医疗保健提供商面临的最大的网络威胁时，科米回答道：“勒索软件”。



8. 身份

到 2021 年，将有 3000 亿口令需要网络防护。其中包括 1000 亿人类口令和 2000 亿机器口令（物联网）。有些专家甚至估计，口令数量比这最近的预测还要多。



9. 移动

2025 年，WiFi 和移动设备预计将占据近 80% 的 IP 流量；2020 年，该预测数字是 66%；而 2015 年，据思科统计，该数据是 48%。流量态势的转变，将促使 CISO 和 IT 安全团队将更多的资源投入到移动安全领域。



10. 漏洞利用

2015 年到 2021 年，零日漏洞利用将从每周一个，增至每天一个。尽管通过使用自动化和更好的工具，在产出更安全的代码上取得了巨大的进步，但每年产生的代码量是巨大的。而且代码量只会继续呈指数级增长，因为要满足对 Web 应用、移动硬件和物联网设备的软件需求。



11. 代码

2017 年，1110 亿行新软件代码将被创建，它们都需要收到良好防护。IT 安全团队和开发人员疲于应付快速扩大的应用攻击界面——大规模扩张的移动和 Web 应用经济助长了攻击界面的扩大。



12. 人

到 2020 年，有 40 亿人会接入网络，需要网络防护；而去年，该数字是 20 亿。到 2030 年，人类攻击界面可能与世界人口总数持平，也就是 85 亿——当前是 70 亿。



13. 合规

2017 年底，所有美国国防部承包商（约 16 万人左右），都必须符合 DFARS252.204-7012 条例，主承包商和分包商要足够安全。这是驱动 GRC（管控、风险与合规）市场扩张的众多规定之一。



14. 网络攻击

近半数的网络攻击都针对的是小企业。小企业往往没有对员工进行网络风险培训，对商业电邮入侵 (BEC) 骗局毫无防范。FBI 称，BEC 导致的损失已超 30 亿美元。



15. 黑客

一个问卷调查中，65% 的受访者称，黑帽子比白帽子技术娴熟。黑帽子追逐金钱、情报、恶名和不良企图，他们比受到规则限制的白帽子更快、更无所顾忌、更有经验。（新闻来源：中国金融智库综合）



大数据产业的“生力军”



5月17日，由工信部指导，中国通信学会主办，中国电信、中国移动、中国联通、中国铁塔协办的2017年世界电信和信息社会日大会在京举行。今年大会以“发展大数据、扩大影响力”为主题，围绕如何引导信息通信行业提升大数据技术和产业发展水平、服务数字经济发展等问题进行了探讨。

“万物互联”时代正在到来

当人们打电话、发微信、刷微博，以及阅读、购物、看病、旅游时，也在不断产生新数据，堆砌着“数据大厦”；

而通过大数据分析，可以预测交通路况实况，了解客户信用……如今，大数据风暴已席卷生活的各个角落。

“数据就像农业社会的土地、工业社会的能源一样，成为信息社会最重要的生产要素和资源。”中国联合网络通信集团有限公司副总经理姜正新说，大数据不仅在你我身边，而且还在引领生活的新变化。

研究显示，我国的数据总量正在以年均50%以上的速度持续增长，预计到2020年在全球的占比将达到21%。产业新形态不断出现，催生了个性化定制、智慧医疗、智能交通等一大批新技术新应用新业态。

工信部总工程师张峰指出，当前，全球范围内以大数据、云计算、物联网等为代表的新一代信息通信技术发展迅猛，移动互联网、智能终端、新型传感器快速渗透到地球的每一个角落，联网设备产生的数据量呈几何级数增长，“未来，占有和利用数据资源的能力将日益成为国家综合竞争力的一个重要组成部分”。

大量数据仍在各个角落闲置

今年初，工信部发布的《大数据产业发展规划（2016—2020）》提出，到2020年，要培育一批大数据骨干企业、核心龙头企业和若干专业化的数据服务创新中小企业、大数据应用及服务企业，基本形成“技术先进、应用繁荣、保障有力”的大数据产业体系。

“大数据可提供人流预警、公交道路等服务，为公交管理、游客出行提供参考。”中国移动通信集团公司副总经理李正茂说，发展大数据的根本目的是为了应用。

在中国电信集团公司副总经理高同庆看来，当前以大数据、云计算等为代表的现代信息通信技术，正在引领新一轮的产业革命，催生出极具创新力的各类应用产品，激发出全新的商业模式，并不断孕育出新的产业，培育出新的经济增长点。

然而，“我们也清醒地意识到，大数据的发展才刚刚开始”。姜正新提到，我们城市中的数据利用率仅为0.4%，大部分数据还在政府手里或者各个角落闲置，“就我们电信运营商本身，价值数千亿元的数据尚未得到变现”。

姜正新认为，在运营时代，电信运营商不仅拥有庞大的网络和信息基础设施，也拥有大量的数据资源和用户资源，“毫无疑问，电信运营商应成为大数据产业的生力军”。

张峰表示，将推动全国一体化的国家大数据中心建设，引导大数据基础设施向绿色集约、规模适度、高速互联的方向发展。推进公共数据开放和基础数据资源跨部门、跨区域共享，建设覆盖全国的国家大数据中心网络和政府数据开放平台，优先推动信用、交通、医疗、卫生、就业、社保等领域的数据集向社会开放。

建立健全网络数据安全管理体系

从5月12日起，一款名为“Wannacry”的勒索病毒大规模入侵全球电脑网络，波及近100个国家，产生了较为严重的网络安全威胁。

“大数据为信息通信业的发展开辟了广阔空间，同时也要求我们更加注重数据安全，积极参与国家相关政策法规的制定，着力打造数据管理、平台运营、服务应用全方位的安全体系。”高同庆说。

姜正新提到，中国联通将通过与各行业的紧密合作，推动“大数据+”的发展，并建立完善的大数据安全管理体系，重视客户隐私的保护，不断优化数据安全体系，确保数据安全和信息安全。

张峰表示，今后要强化安全监管，建立健全网络数据安全管理体系，建立企业数据资源资产化和利用授信机制，严厉打击非法泄露和出卖个人数据行为，维护网络空间安全以及网络数据的完整性、安全性、可靠性。同时，强化数据资源在采集、存储、应用和开放等环节的安全保护，不断提升网络数据技术防护能力，加强大数据场景下的数据防窃密、防篡改、防泄露、数据脱敏、关键数据审计、数据备份等安全技术的研发和部署。

（新闻来源：光明日报）

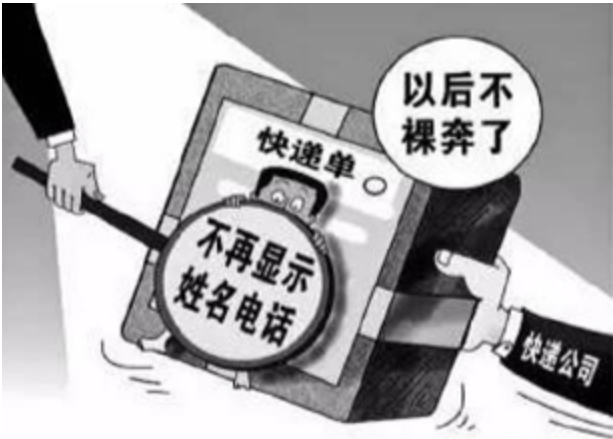
快递行业举行首个信息安全峰会 “隐私面单”让个人信息不再“裸奔”



“剁手族”们在拆完快递后，大多会做一件事，就是将快递面单上的个人信息消除，避免泄露个人隐私。从快递行业首届“御建未来——信息安全峰会”上获悉，随着多家快递企业开始启用“隐私面单”，个人信息将不再“裸奔”。

快递面单潜藏信息泄露风险

近年来，写有收件人姓名、手机号、住址等个人信息的快递面单，已成为泄露个人隐私的“快速通道”，出售快递面单信息已经成了贩卖个人信息的新途径。



公开报道资料显示，2016年4月，合肥一家快递企业的快递员以每张0.8元的价格出售快递面单；2015年底，广东一家快递企业员工，在一个月内向他人出售客户运单信息约1.5万条，获利近2万元；2014年9月至11月，上海犯罪嫌疑人鞠某非法侵入快递公司服务器，下载快递面单信息3万多条，出售他人非法获利逾3万元……

国家邮政局日前发布的今年一季度中国快递发展指数报告显示，一季度全国快递业务量达到75.9亿件、同比增长31.5%；日均快件处理量8433万件，人均快件使用量为5.5件。小小一张快递面单潜藏的个人信息泄露风险，已经成为全民关注的“大事件”。

包裹上的个人信息越来越少

快递行业首个信息安全峰会在深圳召开，跨行业信息安全联盟成立，顺丰、腾讯云、万科物业、申通、韵达、唯品会等知名企业率先加入。

峰会上，顺丰首次对外披露已经开始试点的快递端对端信息安全解决方案。顺丰控股变革管理部负责人官力表示，顺丰已经在部分地区开始试点新版“丰密面单”，除了原本姓名、电话等敏感字段隐藏外，客户的地址信息也将由编码代替，在快递面单上完全实现个人信息加密化。

此外，包括快递员、客服人员等企业内部可能接触到用户隐私信息的环节也进行全流程隐藏，确保用户的信息安全。客户收件时使用“电子签收”功能直接在手持终端上签收，安全环保，有效避免快递纸质面单销毁不当带来的信息泄露隐患。

“‘隐私面单’只能保障部分环节。信息泄露不仅仅在快递运输过程中，因此建立一个全流程的面单信息管理机制十分重要。”在业内人士眼中，顺丰将全国所有建筑逐一编码，相当于创造了一种让外人看不懂的语言，将地图、物流、大数据、环保等诸多领域进行融合，实现了跨维度的交换握手；而收派员、客服人员等企业内部的信息全流程隐藏，为快递乃至整个物流行业提供了一套全新的信息安全解决方案。

除了顺丰外，菜鸟网络联合EMS、百世快递、中通、申通、中国邮政集团公司、天天、德邦、圆通、韵达等快递公司，推出新的“隐私面单”。菜鸟网络安全部高级专家周磊介绍，消费者的信息通过技术处理，不显示在快递面单上，同时在后台也进行了加密处理，快递员只能通过APP联系收件人，无需人工识别手机号码。“我们暂时保留了一些地址信息，主要用于帮助快递员核对包裹。”周磊表示，“以后包裹上的消费者相关信息会越来越少。”

此外，京东从去年6月份开始试行“微笑面单”业务，利用技术手段从包裹生成时即将用户部分信息以笑脸符号隐藏。经过近一年的改善和优化，该服务已在全国范围内推广应用。（新闻来源：新快报）

媒体专访 | 绿盟科技 2016 年报综述： 亿赛通顺利完成业绩承诺



北京亿赛通总经理崔培升先生

从 2014 年绿盟科技收购亿赛通 100% 股权，到 2015 年亿赛通完成业绩净利润 4932 万元，2016 年销售收入达 1.42 亿元，净利润 5507 万元，同时在客户发展上超过万家企业，终端活跃用户过百万，2016 年，亿赛通以 19.2% 的市场占有率，位居中国数据泄露防护市场第一名。

2014 至 2016 的三年时间里亿赛通在渠道建设上不断扩大规模、在产品体系上严把质量关、在技术上开拓创新、在市场营销方面加大投入力度，一系列的重大变革和稳扎稳打的战略布局，亿赛通已完成对绿盟科技并购下的业绩承诺，向绿盟科技交了一份满意答卷。

年份\	2014 年\	2015 年\	2016 年\
销售额 (万元) \	11174.56\	12572.88\	14240.5\
净利润 (万元) \	3278.07\	4932.55\	5506.85\
增长率\	-\	12.5%\	11.3%\

图表：2014-2016 年亿赛通实际销售业绩

“近年来数据安全事故频发，数据安全逐渐被各个领域所重视。在此背景下，数据泄露防护技术和市场获得了快速发展。未来我们将体现数据安全的技术前瞻性和引导性，把加密技术和 DLP（数据泄露防护技术）逐渐融为一体，将数据安全技术产品进行整合，用心做中国数据安全‘防护专家’。”北京亿赛通科技发展有限责任公司总经理崔培升如是说。

全面落实新渠道政策

4 月是万物复苏蓬勃发展的季节，亿赛通在广州、武汉、上海、东北分别举办渠道大会，激发了不少亿赛通代理商的斗志，代理商也纷纷表示，与亿赛通合作对做好 2017 年国内数据安全市场拥有很强大的信心。

2016 年是亿赛通的渠道深耕年，覆盖了不同行业和空

白区域。亿赛通采用扁平化的渠道体系进行结构化管理，全国市场划分为七个大区，每个大区有渠道专属负责人，所有渠道伙伴直接面向渠道经理，在每个省份或直辖市招募金、银牌及钻石代理商，大力开拓数据安全市场，推广文档加密、智能加密和基于内容识别的数据泄露防护整体解决方案。为了增强代理商的合作粘性，亿赛通改变以往的渠道返点政策，直接让利渠道，根据渠道进货量递减进货折扣，充分保证渠道的合理利润。

据崔培升介绍，从 2016 年 3 月开始，亿赛通就全面落实新的渠道政策，改变了过去的渠道散乱局面，处罚并公布有些代理商和管理人员勾结导致的特价行为，营造了公平竞争的环境，让代理商省事、省心，给代理商更大的盈利空间。随着去年 7 月 1 日亿赛通全国渠道大会在北京举行，招募全国百余家合作厂商，在价格方面进行调整制定一些激励政策；培训代理商，使之更专业；100 多家代理商纷纷建言献策，让亿赛通的渠道畅通，能够根据客户的需求对产品进行灵活调整。

打造数据安全产品体系

据崔培升介绍，信息化时代的企业都在最大化地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。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以电子邮件、文件传输等形式轻而易举地流出企业。亿赛通可以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，控制企业内部人员的主动或非主动的泄密风险，从源头上保证涉密资料的安全，避免其他内网安全软件的各种漏洞。

亿赛通的数据安全防护体系主要分为 1 个体系、6 层防护和 20 大应用来提供企业数据保障，跟竞争对手相比，亿赛通的产品链最为丰富。亿赛通正全力打造云服务平台、终端数据防护、网络数据防护、介质数据防护、存储数据防护、

应用数据防护等六大产品体系。

亿赛通的视频数据安全防护系统已经成为数据安全行业的一个“拳头产品”，在文档安全面临的各种数据安全威胁的状况下，其实很多视频数据安全也面临着极大的安全威胁，如公安视频监控数据、生产车间视频数据、办公视频数据等等，这些新的趋势和现实需求对数据安全企业有着更高的技术要求。据崔培升介绍，亿赛通对太原市公安局工作人员所存储的视频文档进行了择优方案部署，促进了太原市公安局视频信息管理更加智能化、有序化，着实提高了太原平安城市的管理化水平；在株洲市公安局广泛应用视频监控系统，对全网视频平台进行防护，既保证了株洲市公安局工作网络较高的可用性、可靠性、保密性，又对核心视频数据有较强的防御、管控能力。

2016 年 12 月，亿赛通又与上海海关数据中心合作项目进行了验收，亿赛通目前已经和国内 49 个海关建立合作关系，帮助海关进行智能识别、动态加密，实现加密数据无感知、加密数据脱离使用环境无法读取、非法获取数据后无法使用，全方位保障海关数据安全。“并且做到敏感数据可保护、安全态势可度量、安全事件可追溯，实现一体化智能防护”。当前，亿赛通已经帮助党政机关、运营商、金融行业、能源电力、制造行业、设计行业、研发通讯行业、医药行业等超过万家企业和超过百万的终端用户提供技术支持。

当被问及对国内的数据安全行业发展的见解时，崔培升认为，拥有和人信息和企业信息的单位都应当把安全保护数据信息的责任担起来。“个人信息作为受保护对象已经写入《民法总则》，并对今年六月实施的《网络安全法》希望加大执法力度，对破坏信息安全的个人或是组织加强严管，让他们受到应有的处罚，彻底从法律层面保护个人信息、企业信息安全。而在数据安全技术上，亿赛通愿和业内同仁共同打造全方位保护的数据安全防护体系，全方位保护各行各业的信息安全，努力降低客户信息安全防护成本投入、更方便地获得优化的数据安全防护产品。”崔培升如是说。

活动会议 | 亿赛通出席 2017 年湖北省勘察设计协会交流会 建立可持续发展信息安全管理体系



亿赛通讯：为深入贯彻党的十八大精神，落实《“十三五”工程勘察设计行业信息化工作指导意见》，积极推动湖北省勘察设计行业信息化建设，5月4日至5日在湖北省举办了“2017年湖北省勘察设计行业信息化工作暨信息技术交流会”。

确保国家秘密安全，维护国家利益不受到损害，保护勘察设计行业知识产权、专利成果和设计方案等商业秘密的安全，不发生任何失泄密事件，以有效保护员工知识性劳动成果，亿赛通作为业内权威的数据安全防护专家，应邀出席了本次信息技术交流大会。为提高行业经济效益是配合院安全保密工作顺利进行的重要工作，亿赛通安全专家和与会人员深度交流探讨了：如何保护好勘察院设计行业信息安全问题？以及与大家共同分享了亿赛通优秀丰富的数据安全解决方案、优秀的经典案例。让勘察设计协会参会人员的信息安全技术有了新的认识。



勘察设计院实现新改制 加强信息安全保护

大会上，亿赛通安全专家详细的分析了勘察设计行业的当下发展情况。近年来，在互联网、大数据等新型时代发展大背景下，信息化之路成为行业发展的必然之道。而国内勘察设计行业也由旧的发展体制进行新的改制。即所在科技建院、科技兴院和可持续发展的方针指导下，大力推进信息化建设，以信息化带动设计院的现代化建设。但是，在新的体制下使得行业的竞争也愈加激烈，如何提升企业竞争力？知识产权、研发数据、设计图纸等等这些不仅是企业的一笔巨大资产，更是市场的核心竞争力。对此，设计院行业高度重视数据安全保护。

部署最佳数据安全解决方案 提升核心竞争力

由于设计院所的人员构成、业务流程和数据的流转都十分复杂。并且面临着十分严峻的挑战，如项目信息泄露、项目交付时出现问题、员工工作时间干私活、机密信息泄密等问题。那么，通常勘察设计院行业针对典型的数据盗窃安全威胁，使用外部防御措施。但是，这些系统的设计无法防止内部人员进行关键信息的盗窃，一般来说，保护内部信息的安全措施通常只允许授权人员访问数据，但此类访问并不授权用户将企业的数据向外泄露，而现有解决方案不能适当地防止此类风险。因此打造内网数据安全体系势在必行。

亿赛通针对设计院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实现设计相关应用系统的数据安全防护要求，实现终端和应用系统数据的安全交互。系统兼容多种应用层协议，对于基于标准网络协议的常见应用系统都能提供完美支持，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。并且提高设计企业核心数据的内部安全管理能力，提高安全事件处理的有效性，降低设计院企业核心数据传输过程中的安全风险，保障数据生命周期的安全，支持设计院企业业务发展和信息化改造过程中数据整合的安全管理，建立可持续发展的信息安全模型。

（新闻来源：亿赛通华中大区）

比特专访 | 亿赛通： 书写数据安全领域新版图



北京亿赛通总经理崔培升先生

拙别喜欢一部西藏文艺片，里面的情节是这样的，聪明的男主角，发现每年来村子里收粮食的人要了滑头，秤上做了手脚。用智慧揭穿了这个骗局。收粮食的大户，为此气愤的拒收全村人的粮食，无奈之下，男主角另寻渠道，走出了一条新的“商路”，并带领全村发家致富。

由此可见，“渠道”无论放在哪儿，放在何时何地都是“发家致富”的通路。对于一个企业而言更是如此，渠道是企业长足发展的必然。在今天云时代下，面对越来越扁平的渠道架构，越来越透明的渠道利润，“渠道”依然有TA的价值体现。无规则不成方圆，如何管理渠道，如何发展渠道，规范和管理是让渠道长足发展的最大推动力量。亿赛通总经理崔培升凭借多年在安全领域积累的经验，将亿赛通的渠道进行了一次大整合，并做了重要规划。

商路多崎岖 唯坚持不懈才能赢市场

外界普遍认为，2016年是中国网络安全的又一元年，信息安全产业在国家政策的指导下突飞猛进。在这一年中，信息安全事件层出不穷，从信息泄露到重大漏洞，从市场变化到把国家安全提上日程。互联网恶意攻击不断演化，无论是国家信息安全、商业机密或是个人隐私都已经发展成为信息泄露事件的重灾区，这直接拉动了国内信息安全产业采购需求的高速增长，也为亿赛通战略向纵深发展开辟了大展拳脚的舞台。

实际上，笔者在同崔培升的交谈中，可以深刻的感受，亿赛通的快速发展，并不只是市场火爆的一个顺势而为。实际上，当2014年绿盟科技收购亿赛通100%股权之后，亿赛通在很长一段时间内都处在舆论的漩涡之中，2015年，亿赛通在完成业绩净利润4931万元之后，再次发力，到2016年亿赛通整体创造了1.42个亿的销售业绩，净利润达到5506万元，顺利完成对并购后的各项任务指标。

如此快速的成长，自然离不开崔培升的稳步布局。一方面，有规划、有步骤的进行市场销售体系的建设，另一方面，构建良性的渠道市场环境。通过这样两步走路线就是崔培升的规划秘诀。

“2016年上半年亿赛通对其销售体系进行了重构，目前客服服务中心分为七大区，覆盖全国28个省4个直辖市，总部设在北京，在每个省会城市都有独立的服务中心为客户提供技术支持和产品服务。如此，改变了过去较为松散的状态、执行力将更为迅速。”崔培升介绍说。

于此同时，拥有一个稳定健康的市场销售体系和前瞻性的关键技术也是必不可少的。2016年年终，崔培升决定大力整合现有渠道，将原有渠道进行再次整合管理，并制定出渠道拓展建设规划，在整个市场上加大对渠道的投入。同时在技术领域，互联网、大数据、云计算、人工智能等成为当下行业发展的新趋势，亿赛通一直坚持“创新”的理念，结合互联网、大数据、人工智能等新趋势开发出极具前瞻性的尖端技术，整合所有终端模块形成一个统一管理平台，对数据进行智能识别、智能审计、智能加密定密，充分运用智能加密技术，率先在同行业的技术水平中占领高地，从而促使企业不断创立了一座又一座新的里程碑。

市场在扩大 唯发展和渠道强基准

于是，崔培升快速制定了渠道体系，划分行业代理、区域代理，开始进行全国渠道，截至目前，亿赛通已经在全国三十余个主要城市设立了分支机构，覆盖全国的营销及服务战略型布局基本完成。

今年，崔培升计划将渠道巡展继续规模化，覆盖所有已经深入的大区，努力完成在行业市场的突破、地市业务

的创新。“以省级总代为核心的渠道营销体系框架已见效果，渠道业务保持在50%增长速度。”从崔培升的阐述中，便能看到渠道体系的建设已经成为了亿赛通稳步前行的基石。

当然，伴随着亿赛通同全国招募的近百家渠道的合作开展，规范的渠道政策和渠道管理方式也在逐步成型，而吸引渠道合作伙伴的最大动力集中在三点“好产品、好价格、好服务”。

合作促发展 唯有合理的资源优势

“产品好、渠道好、服务好，更增加了培训关怀”便是崔培升为渠道设置的优势资源。在价格方面进行调整制定一些激励政策；主要围绕三个方面：“赚钱：能够帮助代理商赚大钱；”省事：亿赛通的品牌影响力和技术能力；省心：亿赛通管理规范，支持到位。”除了这三点之外，“培训代理商，使之更专业。”——崔培升如是说

从管理上看，亿赛通确实有着非常严格的规范制度，完备的报备机制，合理的释放机会，完善的渠道保护商机策略，让很多代理商都感受到了亿赛通的人性化渠道政策。

从渠道商反映来看，“品牌+管理”就是渠道看中亿赛通的最大优势。确实，成立于2003年的亿赛通14年来一直专注在数据安全，在业内的知名度和口碑无论在渠道还是客户端都是毋庸置疑的。

从产品上看，亿赛通的数据安全防护体系主要分为1个体系、6层防护和20大应用来提供企业数据保障，跟竞争对手相比亿赛通的上下产品链最为丰富。14年来，经过了风风雨雨，亿赛通依然坚持过硬的产品和一流的服务方针。而在客户积累上，14年来，亿赛通拥在通信、金融、政府等领域都已经建树颇深，近年来，亿赛通也同很多云服务厂商合作，共同开拓新型数据安全战场。以至于，今天，我们仍能看到亿赛通持续的研发投入推动着企业不断的推陈出新。

因此，未来，随着亿赛通渠道的不断壮大，其产品和服务的不断创新和升级，都将助力合作伙伴在快速增长的安全市场上获取更大份额。显然，作为发展渠道核心力量，已贯穿到亿赛通渠道战略之中，其势必向行业纵深发展，另一方面，亿赛通也将协助渠道商深挖行业需求，为客户提供更优质的服务。

智网络·汇安全

亿赛通携手绿盟科技出席

“智慧安全 2.0” 全国巡讲活动



5月19日,由绿盟科技举办的“智网络·汇安全”绿盟科技智慧安全 2.0 全国巡讲活动在长沙成功举办。围绕“智网络·汇安全”的主题,中国数据安全防护专家亿赛通出席了本次巡讲活动,并向与会的各位嘉宾分享了新一代信息安全架构、建设思路,以及信息安全未来发展的方向探讨。互联网、大数据、人工智能、云安全等新的发展趋势迅猛,那么面对时代背景的大挑战和客户发展的新需求,数据安全企业如何迎合时代,挖掘市场发展潜力不断提升自我,把握时机?



优化渠道建设 打造智慧安全 2.0

当前以大数据、云计算、人工智能为代表的现代信息通信技术,正在引领新一轮的产业革命。大数据能够催生极具创新力的各类应用产品,尤其激发了数据安全行业全新的发展模式。那么,如何把握发展时机?亿赛通的精英伙伴针对渠道建设方面,与参会的各位渠道商进行了深入的探讨和研究。《网络安全法》即将在6月1日起开始实施,在政策的大力支持和鼓励下,亿赛通结合大数据分析、新时期所研发的智能安全技术、最优化的数据安全解决方案等,通过建设智能化的数据泄漏防护系统,打造一个安全、可信、规范、智能的网络环境,实现对数据的安全管控及泄漏防护保障,全面提升各类新型威胁的识别和防御能力。



部署最优数据安全解决方案 构建智能安全管理体系

针对客户新的发展需求,亿赛通数据安全防护整体解决方案是对用户的“有意”、“无意”两种数据泄漏行为的统一防护,采用“事前防御,事中控制,事后追踪,全面防止泄密”的智能一体化的数据安全解决方案,并且融合“加密敏感数据”、“控制敏感内容流通”、“规范员工访问行为”为主体的核心技术,配合身份识别、权限控制、终端管理、应用集成、智能技术、安全接入以及行为审计等功能,形成一套适合国内信息安全现状及管理目标的全新智能解决方案,最终实现“带不走、打不开、读不懂”的控制目标及效果。从而对信息安全的源头进行控制。



结合内容安全防护、应用系统整合以及业务流程支撑等手段,可满足任意行业用户的安全及管理需求。经过14年的成长及完善,亿赛通数据安全解决方案已经积累了大量的成功实践,对此,企业精英伙伴在会议现场对客户进行了案例经验分享,如军政单位、金融行业、设计制造行业、运营行业、能源行业等等经典案例,在各大行业进行了应用和推广。同时,亿赛通更注重本土化及个性化服务,提倡为企业客户提供“因地制宜、量体裁衣”的数据安全服务,为用户打造出全新的数据全生命周期安全解决方案。

《网络安全法》如火如荼 亿赛通参加 2017 珠海 “互联网 + 时代的信息安全” 论坛活动



《网络安全法》如火如荼，作为时下热议的话题，它的实施将具有里程碑式的意义，即是我国第一部网络安全的专门性综合性立法，此次立法进程的迅速推进，显示了党和国家对网络安全问题的高度重视。对此，5月24日，珠海市科协联合珠海市工业互联网协会成功举办了“2017 年珠海科技人创想梦主题活动——互联网 + 时代的信息安全”论坛。亿赛通作为国内数据安全防护专家，被邀请参加了本次会议，共同剖析了信息安全面临的严峻形势，并探讨各大行业如何利用政策优势、结合技术手段共同保障企业的数据资产安全，提前预知信息安全发展趋势。



全力支持政策实施 共同净化网络安全环境

论坛大会期间，亿赛通的专业人士和与会嘉宾探讨到政策优势，长期以来，社会各界十分关注网络安全，强烈要求依法加强网络空间治理，规范网络信息传播秩序，惩治网络违法犯罪，使网络空间清明起来。全国人大代表也提出许多议案、建议，呼吁出台网络安全相关立法。对此，《网络安全法》也将于2017年6月1日开始正式实施，各大行业拭目以待。那么，亿赛通做为国内专业的数据安全防护专家，在网络安全领域具有极大的权威性，帮助众多行业客户实现了技术层面的信息安全保护，打造真正意义上的综合信息安全解决方案。所以，保护信息安全，亿赛通全力支持国家政策，共同净化网络安全环境。



保护网络安全 加强智能数据安全技术投入

保护网络安全，不仅需要政策的支持，更需要结合技术共同防范。讲到技术防护层面，亿赛通资深顾问为现场的嘉宾详细的、透彻的分享了亿赛通智慧网络安全解决方案，以“疏、堵、管、控”的理念为方针，综合互联网、大数据、智能技术、云安全、移动电话网、固话网络等主流通信渠道的信息审计功能于一身，采用先进的行为、内容、模式、声纹等识别技术，结合智能的信息干预等手段，对不良信息传播、网络犯罪等进行有效管控。有效支撑国家信息空间管理业务，提升国家公共安全工作的发现、管理能力与处理效率，为国家安全贡献重要技术力量。

新闻来源：亿赛通华南大区

与其亡羊补牢 不如阻断根源



世界太疯狂 勒索软件炸伤 BOSS 强大内心

最近，各大企业 BOSS 一脸沮丧捶胸自问：噫吁嚱，危乎高哉，经营企业之难难于上青天啊！防！防！防！这个世界太疯狂了！病毒、蠕虫、木马、后门、流氓、广告、钓鱼、炸弹、间谍、垃圾 如今，又多了个勒索，360 度无死角各种防，还是防不过这个互联网时代的各种新的攻击套路。近日的勒索软件全球感染事件，全球都在刷热度，每个人都在蹭热度，刷爆朋友圈，在事件爆发后，很多企业也针对勒索软件给出了各种对付的招数，没错，是管用，但是面对此次事件的突然袭击，我们更应该思考的是如何从根源彻底消灭各种攻击软件。

领先技术 从根源消灭各种攻击软件

本次事件的爆发，究其根源面对的对象是数据文件，勒索软件可以无任何顾虑的光顾你的电脑，对数据文件进行加密，加密后随之勒索解密。谈起数据加密，亿赛通十几年都用其对客户的数据进行安全防护，而今，面对反其道的攻击事件，亿赛通决定重拳出击此类恶意勒索软件，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，屏蔽勒索软件读取终端上存储的数据，让勒索软件无论如何变种，都无法接触到用户数据，从而无法加密用户数据，使勒索行为化为泡影。相比其他保护方式，用户无需系统补丁，无需病毒库样本支持，与传统亿赛通电子文档安全产品一样，终端用户无需改变任何工作习惯，真正的从源头上保护用户的数据安全。另外针对没有加密保护需求的用户，此功能也可以对明文文件进行安全保护。

此功能模块现已对广大新老用户开放，用户可根据自己实际需求选择是否功能升级。或拨打我们服务热线：400-898-1617 进行咨询。功能升级免费哟 ~~~~~

智能驱动 预知风险

亿赛通作为国内专业的数据安全防护专家，一直专注于数据安全防护领域，研发水平在领域中持续突破创新，并且拥有安全行业领先技术和优秀丰富的数据安全解决方案，帮助众多企业搭建了完整的数据防泄露体系，受到各大行业和企业拥护和信任。如今在党政军、能源、设计制造、研发通讯、集团企业、运营商等等领域都已得到广泛实施和应用。

随着移动互联网技术、物联网技术、大数据安全、云安全等信息技术的快速发展和演进，信息安全未来的重点将转向智能驱动的信息安全方向。那么，面对这些新的发展趋势和新问题的不断诞生，亿赛通利用大数据分析、智能安全手段将研发出更加先进的智能安全防护产品，解决各种数据安全问题，从而能够感知风险，抵御未知高级网络威胁的风险，信息安全技术也将更趋碎片化和专业化。

温馨提示

从源头消灭勒索软件，免费功能升级，欢迎拨打服务热线：400-898-1617

老干妈重大商业机密遭窃取？ 泄密真相引发各大 BOSS 深思 溺宠的企业骨干是否割爱留一招？



老干妈牌油制辣椒无人不知的贵州地区传统风味食品之一。工艺精心酿造，具有优雅细腻，香辣突出，回味悠长，是居家必备。然而，老干妈工作人员发现本地另一家食品加工企业生产的一款产品与老干妈品牌同款产品相似度极高。该事件引起了老干妈公司的警觉，公司相关人员认为此现象很可能存在重大商业机密的泄露。



揭秘：内部员工利用职务之便“拿”走企业“机密”

通过相关调查结果，有人非法披露并使用了老干妈公司的商业机密。如此核心的企业机密泄密源头发生在企业内部，是老干妈公司离职人员 A 某。2003 年至 2015 年，A 某历任老干妈公司质量部技术员，工程师等职，掌握老干妈公司专有技术、生产工艺等核心机密信息。2015 年 11 月，A 某以假名做掩护在本地另一家食品加工企业任职，从事质量技术管理相关的工作。

涉嫌商业秘密泄露的案件中，大量的证据均是以电子文档的形式存在的，其证据一般都是随身携带。并且 A 某随身携带的移动硬盘及内含的电子证据资料，并在其台式电脑中发现大量涉及老干妈公司商业秘密的内部资料。

BOSS 揪心企业溺宠骨干 十八般武艺是否留一招？

老干妈引发的这起商业泄密事件，引发各大企业的 BOSS 反思，信任的企业骨干精英需不需要防备泄密行为？小编突然想到老虎拜猫为师的故事，老虎跟猫学习本事，猫十八般武艺样样精通。老虎拜猫为师之后，猫治学严谨，加之教学有方，一方一法，一招一式都严格要求，严格训练，十八般武艺有十七般老虎都学得很好。最后还有一般武艺没有传给老虎……从此以后，普天之下的老师带徒弟都要留一手。

亿赛通小贴士在这里也特别提醒各大企业，80% 的泄密行为都是来自企业内部，所以企业必须高度重视来自内部的威胁，加强防范和加密技术投入。

小贴士亿赛通经典案例 独家干货分享

亿赛通作为中国数据安全防护专家，14 年品牌铸造，携手众多行业如医药行业、地产行业、教育行业、烟草行业、物流、食品等等行业为其数据安全保驾护航，从而助力企业更加有效、有序的管理企业资产，为企业带来更多经济利益。

《网络安全法》6月1日起即刻实施 这些“安全”知识 You 必须 get 到！



《网络安全法》今年6月1日起即将实施。它将如何为个人信息安全保驾护航？又将为企业带来哪些影响？我们拭目以待。但是，网络安全预防知识你不得不知道。

信息泄露途径需注意啥？

警惕 1：公共场所 WiFi 慎连

在公共场所你有没有连接过那些陌生的无线呢？说“NO”的同志，小贴觉得不科学，因为你有“万能钥匙”，因为你生活在一个“蹭吃”、“蹭喝”、“蹭 WIFI”的时代，因为消耗大量流量你伤不起啊……各位宝宝注意了，知识点来了！！！黑客通过建立无线热点窃取接入终端的重要信息可以说是轻而易举，你的银行卡账号密码在黑客的后台如下图赤裸裸显示！

警惕 2：公共充电桩谨慎使用

黑客通过获取充电用户的手机权限，能够深入到用户终端，对用户的个人隐私神不知鬼不觉的进行窃取。

警惕 3：非法网站木马纵横

有些色情淫秽网站、中奖网站等比比皆是，当你真的进入链接进行浏览时，你的电脑或者手机将有很大的几率被植入木马，个人隐私也就没有什么安全可言。

警惕 4：诈骗短信横行霸道

虚假短信链接千万不要随意点，一旦点击链接，就有可能中招，个人隐私安全问题堪忧！

警惕 5：软件获取最高权限窃密

很多软件都会对手机权限进行获取，权限访问时，请理智分析，注重隐私保护！

警惕 6：朋友圈、微博晒照需谨慎

晒个人信息在你的眼中可能没有太多的利用价值，但一代落入别有用心的人的手中，对于你来讲可能是一场“灾难”。

保护信息安全如何做？

- 首先，
加强个人信息保护 规范个人信息收集；
 - 其次，
个人信息泄露 网络运营者要告知；
 - 第三，
打击网络诈骗；
 - 第四，
依法“网络实名” 网络运营者不得为非实名用户提供服务；
 - 第五，
对网络服务提供者要求更高，开展业务同时需保障安全。
- 中国数据安全防护专家亿赛通特别提醒大家：无论个人或企业需增强信息安全防护意识！

防范和化解敏感信息泄密风险

亿赛通携手长城证券

建立信息防泄露体系



关于长城证券

长城证券有限责任公司，成立于 1995 年 11 月。公司现注册资本 20.67 亿元。股东分别是中国华能集团公司、深能源、招商局、中国核工业集团公司等国内知名大型国有企业集团。公司经营范围是为客户提供证券代理买卖、证券发行与承销、收购兼并、改制重组、财务顾问、资产管理、证券咨询等证券投、融资全方位服务。公司控（参）股长城基金管理公司及景顺长城基金管理公司。公司在国内 20 个城市拥有营业部网点 24 家。

需求背景

长城证券服务模式正由传统的柜台服务模式向网上银行、第三方支付、P2P 小额贷款、企业网络融资等新型服务模式扩展。信息化金融已逐渐成为金融业的发展方向。但与此同时，由于这种新型服务方式虚拟化、业务边界模糊化、经营环境开放化等特点，无论是从组织内部还是外部而言，都使得金融业务面临网络攻击、非法窃取交易信息、客户信息泄露等新的信息安全问题。如何利用信息技术优势加强长城证券公司的内部控制，防范和化解敏感信息泄密风险，是当前长城证券信息安全关注的重点和难点。

解决方案

电子文档安全管理系统是一款电子文档安全防护软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止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，对电子文档进行全生命周期防护，系统具有透明加密、主动加密、智能加密等多种加密方式，用户可根据部门涉密程度的不同（如核心部门和普通部门），部署力度轻重不一的梯度式文档加密防护，实现技术、管理、审计进行有机的结合，在内部构建起立体化的整体信息防泄露体系，使得成本、效率和安全三者达到最优平衡，

实现电子文档的数据安全。

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。

内容安全管控：截屏录屏控制文档、阅读水印文档、打印水印、拷贝粘贴控制。

文档权限管理：细粒度权限控制、模板批量授权、文档权限管理。

文档外发管理：用户身份认证、使用权限管控。

流程管理：文件解密审批流程、文件外发审批流程、邮件外发审批流程、离线办公审批流程、文件还原审批流程。

审计跟踪：邮件外发审计、文件解密审计、文件打印审计、流程全文检索审计、违规操作预警。

项目成果

长城证券有限责任公司通过部署了亿赛通文档安全产品保证了文档敏感信息的安全，使得员工在使用过程中内部透明，使用无感知；外部用户非法获取内部文档无法使用；合法用户获取内部文档首先使用。

浦发银行签约亿赛通有效制定安全策略 共铸“数据安全”坚强堡垒



客户简介

上海浦东发展银行股份有限公司（以下简称：浦发银行）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。

中国建设银行携手亿赛通部署 最优数据安全解决方案 保障银行数据无懈可击



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。

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。

中 / 国 / 传 / 统 / 节 / 日

粽情端午

粽香前里
端午你我共同的节日

粽情端午

THIS SUMMER, KEEP YOU COMFORTABLE AND RELAXED
KEEP AWAY FROM THE HOT SUMMER

亿赛通送祝福！

时至五月五，

粽子飘香，

龙舟正舞，

一杯雄黄酒，

一声亲切的问候，

一个真诚的祝福，

采一片清香的粽叶，

包一颗香甜的粽子，

装入真情的粽子里，

亿赛通祝福所有朋友们端午节快乐！

