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

6 月刊

2019 年共 11 期

教育行业也无法幸免，上海交大 8.4TB 电子邮箱数据泄露

喜报→亿赛通 DLP 产品成功入围国家税务总局 2019 年信息化产品协议采购名单

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

刊首语 PREFACE

《亿赛通六月刊》新鲜出炉，带你回顾安全行业大事件

网络时代，国家的兴衰，更多地取决于对数据的生产获取和使用。发达国家凭借先进技术的优势可能使发展中国家沦为新的“网络殖民地”。由此，确立并保持发展中国家网络安全意识至关重要。针对安全厂商而言，其视角也需慢慢变化，不能再满足于概念性的奔走呼号，要化被动为主动，切切实实关注落地时效和响应时效。企业管理者也应充分认识数据安全工作的重要性和紧迫性，加强对本单位、本部门的重要信息系统、数据、工控系统等关键信息基础设施和重点网站梳理自查……

国内

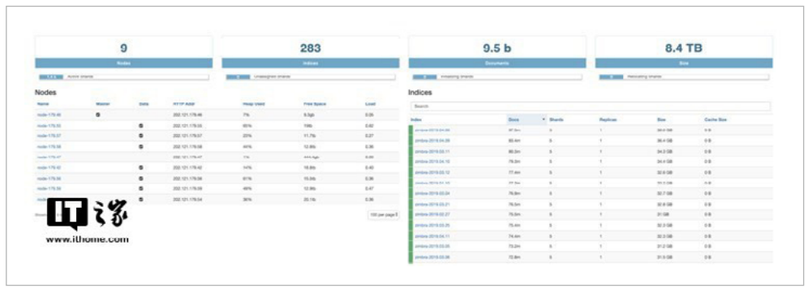
1、中央网信办等四部委联合开展互联网网站安全专项整治，将处罚并曝光违法违规网站

摘要：近日，中央网信办、工业和信息化部、公安部、市场监管总局四部门于 2019 年 5 月至 2019 年 12 月，联合开展全国范围的互联网网站安全专项整治工作，对未备案或备案信息不准确的网站进行清理，对攻击网站的违法犯罪行为进行严厉打击，对违法违规网站进行处罚和公开曝光。

2、浙江开出首张违反《网络安全法》侵犯个人信息罚单：10 万元

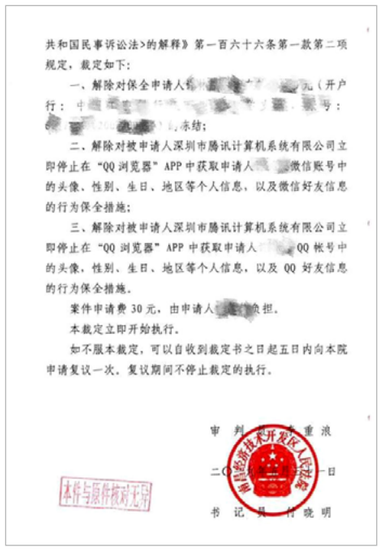
摘要：苍南林某花 1600 多元购入 1000 多个他人注册企鹅号，以非法方式获取侵犯个人信息，违反《中华人民共和国网络安全法》。6 月 3 日，苍南警方对林某处以罚款 10 万元的处罚。这是自 2017 年 6 月 1 日《中华人民共和国网络安全法》实施以来，全省首例因侵犯个人信息违反该法开出的罚单。

3、上海交大泄漏 8.4TB 电子邮件数据



摘要：据博客 Rainbowtabl.es 称，上海交通大学一个 ElasticSearch 数据库因未正确配置公开访问权限，导致 8.4TB 的电子邮件元数据泄露。

4、QQ 浏览器收集用户隐私被法院裁定，腾讯：已解除保全


共和国民事诉讼法>的解释》第一百六十六条第一款第二项规定，裁定如下：

一、解除对保全申请人[redacted]（开户行：[redacted]，账号：[redacted]）冻结；

二、解除对被申请人深圳市腾讯计算机系统有限公司立即停止在“QQ 浏览器”APP 中获取申请人[redacted]微信账号中的头像、性别、生日、地区等个人信息，以及微信好友信息的行为保全措施；

三、解除对被申请人深圳市腾讯计算机系统有限公司立即停止在“QQ 浏览器”APP 中获取申请人[redacted]QQ 帐号中的头像、性别、生日、地区等个人信息，以及 QQ 好友信息的行为保全措施。

案件申请费 30 元，由申请人[redacted]负担。

本裁定立即开始执行。

如不服本裁定，可以自收到裁定书之日起五日内向本院申请复议一次。复议期间不停止裁定的执行。

审判[redacted]重浪

二〇[redacted]一日

书记员[redacted]晓明

本件与原件核对无异

摘要：近日，许先生在江西某法院起诉了“QQ 浏览器”APP 运营方腾讯。因为“QQ 浏览器”APP 在许先生不知情的情况下，窃取了许先生的大量隐私，不仅包括微信和 QQ 的头像、性别、地区、生日等个人信息，还包括微信、QQ 的好友关系信息。而且，在“QQ 浏览器”中，还找不到任何能够删除个人隐私信息的地方。

5、广东：校园学习类 APP 不得随意征集学生家长信息

摘要：近日，中共广东省委教育工作委员会等 7 部门宣布，《广东省面向中小学生校园学习类 App 管理暂行办法》（以下简称管理办法）正式出台，旨在治理学习类 App 存在的诸多问题，进一步规范校园学习类 App 使用。

6、一夫妻联合百余位黑客攻击国内公司，敲诈解密费获利 700 余万

摘要：6 月 21 日，记者从武汉市公安局江汉分局了解到，该局历经 3 个月的侦查，破获一起网络敲诈案，广东一对夫妻在深圳注册两家公司联合黑客攻击国内多家公司的电脑，以解密为由索利，先后获利 700 余万元。

7、虚假的游戏外挂，真正的木马病毒

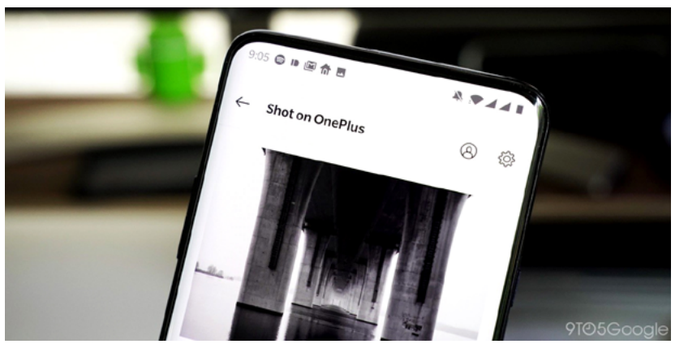
摘要：最近，研究人员发现了一种新的基于 JavaScript 的模块化下载程序特洛伊木马，并通过其开发人员拥有的网站以游戏外挂的形式分发给目标。该恶意木马是由 Yandex 发现的，随后将其发送给 Doctor Web 的研究团队进行进一步分析，并提供了有关如何分发该特洛伊木马样本的其他信息。研究人员发现，这个被称为 MonsterInstall 的特洛伊木马程序使用 Node.js 在受害者的机器上执行命令。

8、实测曝光！京东金融、智联招聘等 24 款 APP 超限索权

摘要：6 月 10 日至 17 日，新京报记者依照《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》中的分类选取了 50 款常用 APP，对其索取的权限以及收集信息的范围进行实测，发现若严格按照《信息规范》中划定的信息收集范围，这 50 个 APP 中有 24 个 APP 索取的权限超出范围，如智联招聘索取了相机、位置、通讯录权限，百合婚恋收集了通讯录权限。

国外

1、首次披露！ OnePlus 一加公司正泄露用户隐私数据，包括地点信息等

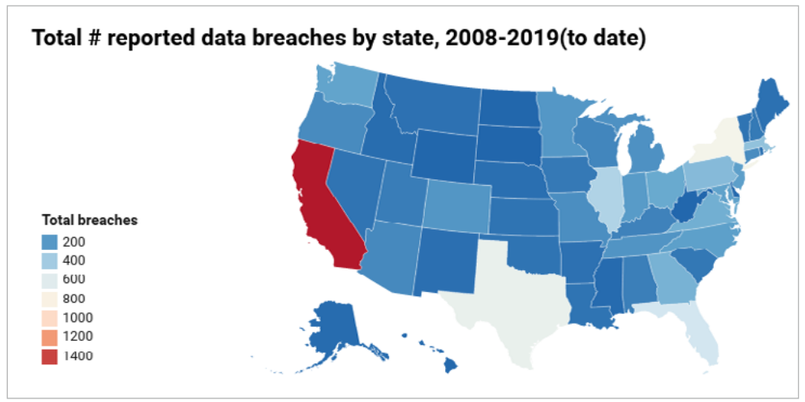


摘要：“Shot on OnePlus”应用程序，可通过壁纸选择菜单访问。顾名思义，它包含 OnePlus 用户上传的照片，允许您将它们设置为当前的壁纸。每天，应用程序中会出现一张新照片。用户可以从应用程序本身或从网站上传照片。在任何一种情况下，都需要登录才能上传照片。用户还可以从应用程序和网站调整其个人资料，包括他们的姓名，国家和电子邮件地址。

2、谷歌扩展插件 Evernote Web Clipper 爆漏洞，允许窃取数据

摘要：Guardio 的研究团队发现了谷歌浏览器插件 Evernote Web Clipper 的一个关键漏洞。Guardio 发布的一篇博客文章写道。“一个逻辑编码错误使得打破域隔离机制并代表用户执行代码成为可能——授予对敏感用户信息的访问权，而不限于 Evernote 的域。”

3、十年间，美国因数据泄露事件损失超过 1.6 万亿美元



摘要：从公共消息来源收集的数据显示，自 2008 年以来美国发生了近 9,700 起违规事件，涉及超过 107 亿条记录，以 2018 年平均成本计算为每条记录 148 美元，粗略计算 10 年里财务损失超过 1.6 万亿美元。

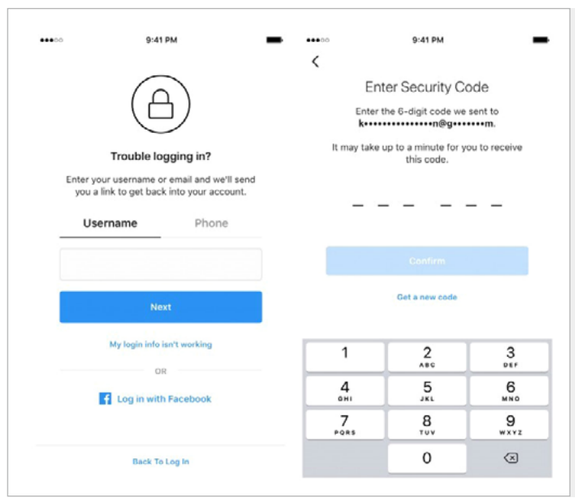
4、美国俄勒冈州人力资源服务部门发生数据泄露

摘要：美国俄勒冈州人力资源服务部门官员证实，该组织在今年 1 月发生了数据泄漏事件，64.5 万名用户的个人详细信息和健康信息受影响。受数据泄露影响的个人参加了该部门的福利和针对儿童安全事件的服务计划。违规行为发生在 1 月 8 日针对该部门的电子邮件”网络钓鱼“攻击中，九名员工打开了该电子邮件，并点击了一个链接，让攻击者能够访问他们的电子邮件帐户，然后进一步访问数据。

5、Firefox 出现严重安全漏洞，建议所有用户尽快更新

摘要：Mozilla 发布了 Firefox 67.0.3 和 Firefox ESR 60.7.1 版本，用于紧急修复最新发现的 0day 漏洞。由于 Array.pop 中的问题，操作 JavaScript 对象时可能会出现类型混淆漏洞。这可能导致可利用的崩溃。该漏洞能够让黑客操纵 JavaScript 代码诱骗用户访问，并将恶意代码部署到他们的 PC 上，安全等级为“严重”。甚至美国网络安全和基础设施安全局也已经参与传播有关补丁的信息。

6、Instagram 正在测试恢复被黑客窃取的帐户的新方法



摘 要：据外媒 Techspot 报道，Instagram 上的网络钓鱼和帐户被盗已成为一个问题，当 Instagram 无法快速帮助用户时，一些 Instagram 受害者通常会求助于白帽黑客。现在 Instagram 正在尝试新的安全技术，这些技术可以让用户更容易重新获得已被黑客攻击的帐户，并且更难以让恶意行为者开始使用帐户。

7、TP-LINK Wi-Fi 中继器出现漏洞，可用于远程代码执行

摘要：IBM 公司研究员近日发布警告称，一些 TP-Link 的 Wi-Fi 中继器设备存在严重的远程代码执行漏洞，漏洞可导致外来攻击者获取设备权限并执行任意命令。IBM 安全顾问指出，除了使被控设备变成僵尸网络的一部分外，攻击者还可以通过在设备连接的操作系统上执行任意的 shell 命令来进行恶意行为。黑客可以通过这个漏洞向所在系统进行横向提权，直到获得管理员权限。

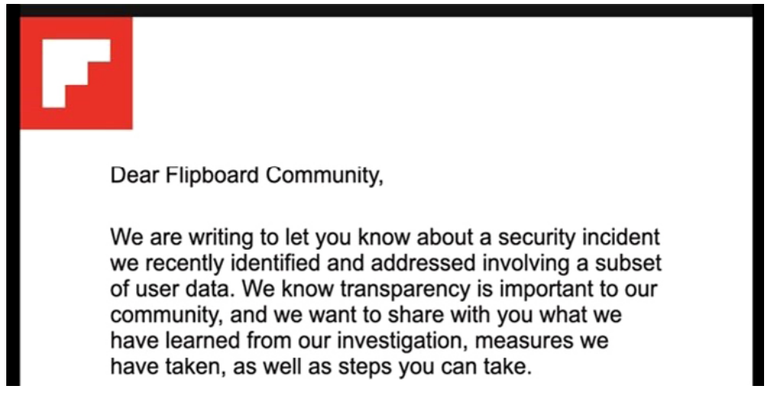
8、新的黑客钓鱼活动以 WSH RAT 为目标银行客户

摘要：安全专家 Cofense 网络钓鱼防御中心已经发现针对商业银行客户的网络钓鱼活动正在分发一个跟踪为 WSH RAT 的新远程访问木马。名称 WSH 可能是指合法的 Windows 脚本宿主，它是用于在 Windows 计算机上执行脚本的应用程序。威胁演员正在使用 RAT 来提供 键盘记录器 和信息窃取者。

9、旅游公司数据泄露导致以色列总理及其家人行踪暴露

摘要： 旅游公司 Amadeus 的以色列数据库遭遇数据泄露，数百万以色列旅行者的私人信息被曝光。据称，整个数据库包含了 3600 万航班预订信息、1500 万乘客个人信息、70 万签证申请和 100 多万酒店预订信息，其中包括以色列总理本雅明内塔尼亚胡（Benjamin Netanyahu）及其家人，以及其他高级官员的飞行行程。

10、新闻聚合应用 Flipboard 内部被渗透超 9 个月，用户数据全泄露


Dear Flipboard Community,

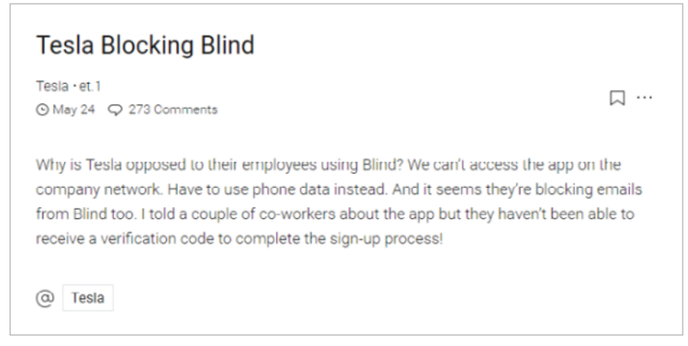
We are writing to let you know about a security incident we recently identified and addressed involving a subset of user data. We know transparency is important to our community, and we want to share with you what we have learned from our investigation, measures we have taken, as well as steps you can take.

摘要：新闻聚合服务和移动新闻应用 Flipboard 发布安全通告，公司内部多个系统遭到黑客攻击，已经持续超过 9 个月时间。援引外媒 ZDNet 掌握的多封电子邮件，Flipboard 表示黑客获得了存储客户信息的服务器访问权限。在该服务器上存储了用户名、哈希值、加密密码，以及和第三方服务捆绑的 Flipboard 个人资料。

11、美国金融公司网站泄露 8.85 亿份敏感数据

摘要：First American 金融公司在网上泄露了数亿份与房地产和抵押贷款行业有关的敏感记录。泄露的数据包括一些高度敏感的数据，如抵押贷款、税务记录、社会保险号、电汇收据、驾照图像、银行账号和对账单等。泄露的信息来自 First American 网站 firstam.com。由于网站缺乏安全措施，任何人无需身份验证即可访问数据。如果知道网站上有效文档的 URL，只要修改链接中的一个数字，就可以查看其他文档。

12、公司信息遭泄露后，特斯拉禁止员工使用匿名聊天应用程序


Tesla Blocking Blind

Tesla · et.1

May 24 273 Comments

Why is Tesla opposed to their employees using Blind? We can't access the app on the company network. Have to use phone data instead. And it seems they're blocking emails from Blind too. I told a couple of co-workers about the app but they haven't been able to receive a verification code to complete the sign-up process!

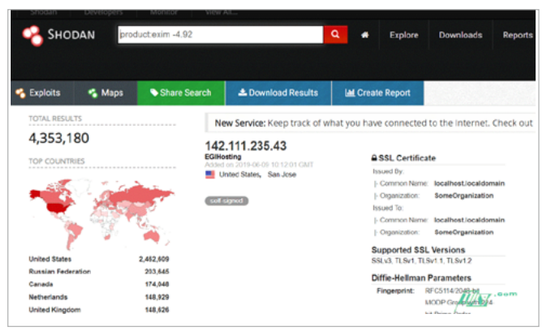
@ Tesla

摘要：据外媒 CNET 报道，Blind 已经确认，在公司消息遭泄露后，特斯拉已阻止员工使用这款匿名工作场所社交网络应用程序。Blind 表示特斯拉正在阻止其员工接收验证电子邮件，因此员工将无法验证其帐户。

13、新的僵尸网络出现，150 多万台 RDP 服务器很危险

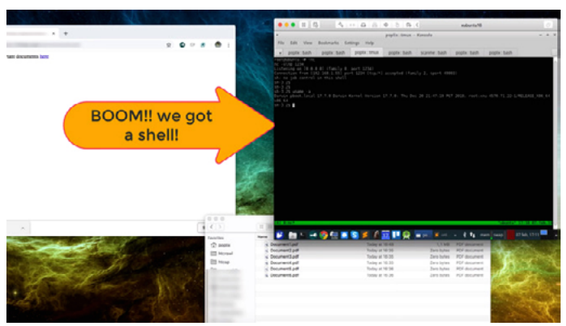
摘要：据外媒报道，一个新的僵尸网络被称为 GoldBrute，扫描随机 IP 地址来检测暴露了 RDP 的 Windows 机器有 150 多万台 RDP 服务器易受攻击。与其他僵尸网络一样，GoldBrute 并没有使用弱口令，也没有利用数据泄露中的重复密码，而是使用自己的用户名和密码列表来发起蛮力攻击。

14、Exim 邮件服务器存在严重漏洞，数以百万计用户受网络攻击



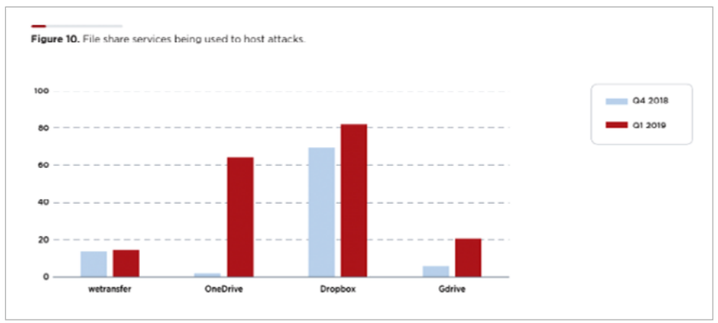
摘要：严重漏洞会影响 Exim 邮件传输代理（MTA）软件的 4.87 到 4.91 版本。未经身份验证的远程攻击者可利用此漏洞在邮件服务器上执行某些非默认服务器配置的任意命令。该漏洞（ CVE-2019-10149）位于 /src/deliver.c 中的 deliver_message（）函数中，它是由收件人地址验证不正确引起的。该问题可能导致使用邮件服务器上的 root 权限远程执行代码。

15、macOS 门禁功能爆出安全漏洞：可安装恶意程序



摘要： 门禁（Gatekeeper）是 macOS 系统上的一项安全工具，旨在确保只有受信任的软件才能在 Mac 上运行。不过援引外媒报道，这款应用身份认证功能存在安全漏洞，可以用于传播名为“OSX/Linker”的恶意软件安装包。

16、安全人员统计 Onedrive 托管的恶意软件季度增长达 60%



摘要：微软 OneDrive 用于托管恶意文件的使用率显着上升。根据 FireEye 报告显示，微软 OneDrive 上一季度托管恶意文件的用户数量激增 60% 以上，而此前仅上升了一位数百分点。据 FireEye 称，OneDrive 在托管恶意文件的使用率方面，已经超过 Dropbox、Google Drive 和 WeTransfer 等竞争对手。

喜报→亿赛通 DLP 产品成功入围国家税务总局 2019 年信息化产品协议采购名单

近日，国家税务总局 2019 年信息化产品协议供货商名单正式公示，亿赛通“数据泄露防护（DLP）系统”成功入围。此次中标“国税系统政府采购信息系统信息化产品入围采购项目”，意味着亿赛通的技术水平与服务能力得到了国税系统的高度认可。

严格审查、精中选优

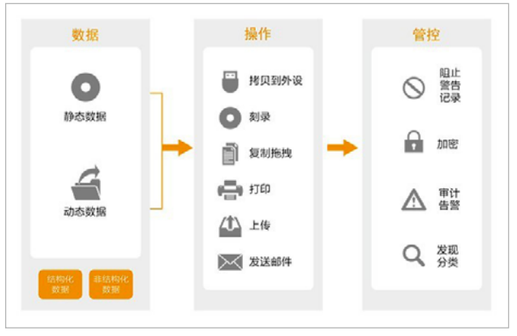
国家税务总局是国务院主管税收工作的直属机构，对信息系统建设要求十分严苛，从产品的稳定性、可用性、兼容性、可扩展性等方面对安全厂商进行严格甄选，信息安全产品作为信息化基础设施的重要组成部分，是整个集采入围活动的重点。据国家税务总局集中采购中心表示，他们除了对产品审核十分严格，在公司资质等各方面的要求更是严苛。

亿赛通自成立以来，始终将党政军用户作为公司重点服务对象，为其提供优质产品及服务。在国家税务总局信息化产品集采入围项目中，我司全程积极参与，提供了优于招标技术要求的信息安全产品，得到国税系统的高度认可。

中标包期	中标产品	型号
第五包计算机软件	数据泄露防护（DLP）系统	V5.0

数据泄露防护（DLP）系统

DLP 系统是基于内容识别技术，对设计图纸、源代码、合同文本、财务报表等敏感文件进行数据安全保护。



产品特性：

1、内容识别：可以通过文件类型、关键字、正则表达式、数据指纹等方法对终端内容进行识别，并可基于中文分词语义进行分析，有效识别敏感文件内容。

2、数据防护：可以对邮件客户端，共享文件，QQ、腾讯通等实时通讯软件进行有效防护，避免通过文件共享、邮件附件、QQ 聊天等途径泄露敏感信息。

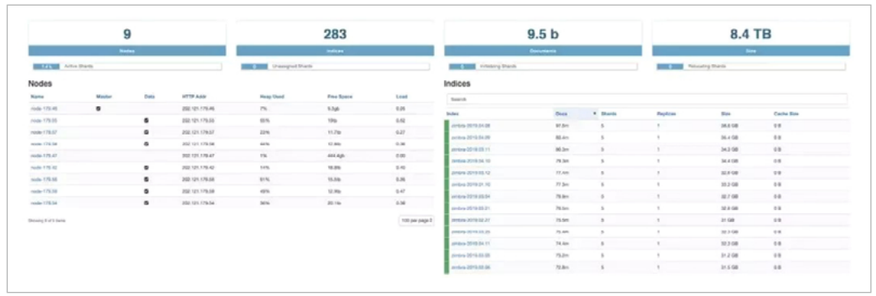
3、端口管控：可对 USB、蓝牙、打印机等外设端口进行管控，禁止通过 U 盘拷贝、打印等途径进行敏感信息外泄。

4、审计分析：可对泄密事件进行分类审计、对比分析。并对趋势进行统计分析。

作为国内一流的数据安全厂商，16 年来，公司用实力证明了自身的产品研发水平与市场拓展能力。并且与多家国家机关单位开展友好合作，为其提供数据安全技术服务，助力其信息安全建设，获得良好的口碑效应。此次公司自主研发的数据泄露防护系统成功入围，在企业资信、产品能力及售后服务体系建设方面彰显了实力，同时也极大提升公司市场知名度与品牌影响力。

在为国家机关单位提供安全服务的同时，亿赛通的用户群体也在不断扩大，越来越多的行业客户选择了亿赛通的产品。未来，我司将继续秉持“服务客户、持续创新、专业至上”的理念，做好中国数据安全防护专家的角色，为用户提供专业化服务。

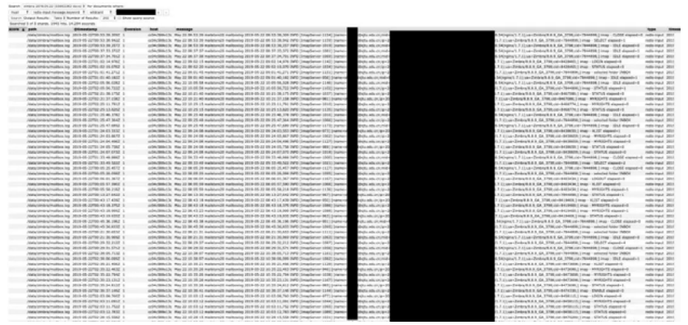
教育行业也无法幸免，上海交大 8.4TB 电子邮箱数据泄露



上海交大 8.4TB 电子邮件数据泄露

日前，根据外媒某安全博客上的文章报道，上海交通大学一个数据库因未正确配置公开访问权限，而导致泄漏了 8.4TB 的电子邮件元数据。

该泄漏数据库包含 95 亿行数据，在发现时处于活动状态，其大小由 5 月 23 日发现时的 7TB，一天后增加到 8.4TB。该数据库属于上海交通大学，这是一个总部设在中国的大型学术机构，学为 41,000 多名本科学生提供博士学位。



数据库中包含的信息是通过 Zimbra 打包的，zimbra 是全球超过 20 万家企业使用的流行开源电子邮件解决方案。根据安全专家的说法，通过这些数据，可以找到特定用户发送或者接收的所有邮件，此数据还包括检查其电子邮件的人员的 IP 地址和用户代理，据此可以找到所有使用的 IP 和特定人员的设备类型。此外，通过这份数据库，还能查到多个特定用户之间的邮件来往记录。

不过，需要注意的是，这份数据库并不包含邮件主题信息以及邮件的正文内容，不然这次数据泄露的威胁程度会更加严重。

在发现泄漏一天后，上海交通大学接到了数据库泄漏的通知。值得称道的是，泄漏在 24 小时内被修复。

安全专家称：校方的安全团队，一接到通知，就迅速采取行动，确保这些数据的安全。不过，就我所知，他们没有通知受影响的学生。

中国数据安全防护专家在此希望学校能对学生诚实以告，让他们尽早采取措施，更改账户密码，也希望相关部门多一份社会责任感，如果他们早一点采取信息安全保护措施、早一点使用安全加密产品，就不会酿成今天的结局，少投入大盈利。所以，无论企业或个人一定要意识到数据安全保护的重要性，提早采取防护措施。未雨绸缪，防患未然。

经典案例分享

北京建筑工程学院

北京建筑大学

华中科技大学

东北林业大学

山东工商学院

同济大学

长安大学

四川外国语大学

中国民航大学

浙江工业大学

中国人民解放军陆军军官学院

文思海辉技术有限公司

达内时代科技集团有限公司

教育部教育管理信息中心

一言不合“秀技术”，再不采取措施就晚了……

作为中国数据安全防护专家，

听到这样的消息，

小亿只想原地爆炸，

没错，是原地爆炸！！！

怎么搞的啊？？？

411 万赎金？？？ NASA 被黑客攻击？？？

后果很严重，很严重，很严重……

美国向黑客支付 411 万赎金以换取记录修复

5 月，美国一政府员工不小心点击邮件中恶意链接，导致 Dropbox 里文件被黑客加密要挟……结果公司整个弃用了 Dropbox。同时黑客借机侵入政府计算机系统并加密了市政府大量文件。

6 月中旬，美国佛罗里达州里维埃拉比奇市 (Riviera Beach City) 市议会一致表决通过了支付赎金的要求，他们认为如果想要取回被加密的记录，这是唯一的方法。

联邦调查局发文称表示“不赞同”向黑客支付赎金，但遭到黑客攻击后，该市已花近 100 万美元（约合人民币 697 万）购置新电脑和其他硬件进行系统和硬件的升级。

该市市政府发言人说，市政府一直与外部安全顾问合作，他们也建议支付赎金，赎金将以虚拟货币“比特币”支付。但她同时承认，即使黑客收到钱，也无法保证他们一定会释放所有资料。

近年来，美国和全世界的许多政府和企业都受到了攻击。美国政府去年因两名黑客涉嫌发起 200 多起勒索软件攻击而起诉他们，其中包括针对亚特兰大和新泽西州纽瓦克的攻击。联邦检察官说，这些尚未被捕的黑客收到的赎金超过 600 万美元，并对计算机系统造成 3000 万美元的损失。

NASA 自曝遭黑客攻击 500MB 火星任务数据失窃

据外媒报道，2018 年 4 月，黑客曾侵入美国宇航局（NASA）网络，窃取了约 500MB 与火星任务有关的数据。

入口点是 Raspberry Pi 设备，该设备未经授权或通过适当的安全审查而连接到 NASA 喷气推进实验室 (JPL) 的 IT 网络上。黑客利用这个入口点通过黑客攻击共享网络的网关，侵入 JPL 网络中，从 23 个文件中窃走了约 500MB 的数据，其中 2 个文件包含与火星科学实验室任务相关的“国际武器贸易条例”信息。

调查人员表示，2018 年 4 月的入侵者除了访问 JPL 的任务网络外，还访问了 JPL 的 DSN IT 网络。在入侵发生后，NASA 的其他几个设施断开了与 JPL 和 DSN 网络的连接，因为担心攻击者也会转向他们的系统。JPL 管理 NASA 的深空网络 (DSN)，这是一个由卫星天线组成的全球网络，用于在现行任务中通过 NASA 航天器发送和接收信息。

NASA 表示：这次攻击被归类为一种高级持续威胁，在近一年的时间里都没有被发现，对这起事件的调查正在进行中。

看完这两件黑客攻击的惨重事件，有网友表示如果他们提前采取严密的数据安全保护措施，就不会酿成今天的悲惨结果。小亿也想说，如果一切都没有发生，小亿一定把超安全的亿赛通数据加密产品推荐给他们，然后，就算黑客发送病毒邮件，就算黑客入侵，数据丢失、窃取、拿走……亿赛通智能加密产品也可以完全防护，让对方无法查看，无法获取。但是，没有如果……不过，现在醒悟也不晚。无论企业或个人一定要意识到数据安全保护的重要性，一定要提前采用数据安全防护措施。

亿赛通智能安全产品，融合大数据分析、文档加密、访问控制、关联分析、数据标识等技术，可帮助用户对数据进行数据治理、态势感知、智能防护，为用户的核心数据资产从终端、网络、存储、应用等全方位提供全生命周期保护，从而做到事前预防、事中控制、事后审计于一体化防护，可效防止重要信息被有意或无意非法扩散，让客户再也不担心数据被泄密、存储不安全。

网信办重磅发布《数据安全管理办法（征求意见稿）》，保障数据安全 亿赛通责无旁贷

近两个月来，网信办动作连连，先后公布了《数据安全管理办法（征求意见稿）》（简称《办法》），《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）》等向有关个人信息保护的征求意见稿。由此可见，一方面，无论是受国际影响还是社会舆论影响，政府层面对个人信息的保护作出回应势在必行；另一方面，个人信息强保护的趋势已经开始显现，尤其是《数据安全管理办法》，更被业界人士戏称为中国的 GDPR。

《办法》以“网络运营者”为主要规制对象，重点围绕个人信息和重要数据安全，在数据收集、数据处理使用、数据安全监督管理等方面进行了系统的规定。作为《网络安全法》核心的配套法律文件，该意见稿广泛吸收国家标准中的成熟规定，对现行数据安全规范体系进行了创新和补强，标志着我国数据安全管理迈出了具有里程碑意义的一步。

主要内容

《办法》的主要内容有总则、数据收集、数据处理使用、数据安全监督管理、附则等五章共四十条内容。重点明确了使用范围、监管主体、个人信息收集和处理、问题处置等内容。

第一，《办法》中明确规定：在中华人民共和国境内利用网络开展数据收集、存储、传输、处理、使用等活动（以下简称数据活动），以及数据安全的保护和监督管理，适用本办法。

第二，监管部门明确：在中央网络安全和信息化委员会领导下，国家网信部门统筹协调、指导监督个人信息和重要数据安全保护工作。地（市）及以上网信部门依据职责指导监督本行政区内个人信息和重要数据安全保护工作。

第三，《办法》要求网络运营者及时处理相关投诉举报，明确了网络运营者在发生数据安全事件时的应急处置要求。并对违反《办法》规定的网络运营者，由有关部门依照相关法律、行政法规的规定，根据情节给予公开曝光、没收违法所得、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照等处罚；构成犯罪的，依法追究刑事责任。

要点解读

《办法》内容比较丰富，针对当前社会关切的数据安全和保护问题都有所涉及，总体来讲《办法》对现有数据安全规则进行了总结和创新，并直面当前热点问题。

第一，收集使用规则应当明确具体、简单通俗、易于访问，突出以下内容：

（一）网络运营者基本信息；

（二）网络运营者主要负责人、数据安全责任人的姓名及联系方式；

（三）收集使用个人信息的目的、种类、数量、频度、方式、范围等；

（四）个人信息保存地点、期限及到期后的处理方式；

（五）向他人提供个人信息的规则，如果向他人提供的;

（六）个人信息安全保护策略等相关信息；

（七）个人信息主体撤销同意，以及查询、更正、删除个人信息的途径和方法；

（八）投诉、举报渠道和方法等；

（九）法律、行政法规规定的其他内容。

第二，网络运营者应当严格遵守收集使用规则，网站、应用程序收集或使用个人信息的功能设计应同隐私政策保持一致，同步调整；收集 14 周岁以下未成年人个人信息的，应当征得其监护人同意；网络运营者不得依据个人信息主体是否授权收集个人信息及授权范围，对个人信息主体采取歧视行为，包括服务质量、价格差异等； 网络运营者从其他途径获得个人信息，与直接收集个人信息负有同等的保护责任和义务；网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

第三，针对当前网络运营者的热点问题作出约束。网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人信息；个人信息主体同意收集保证网络产品核心业务功能运行的个人信息后，网络运营者应当向个人信息主体提供核心业务功能服务，不得因个人信息主体拒绝或者撤销同意收集上述信息以外的其他信息，而拒绝提供核心业务功能服务。

对业界的影响

《办法》明确了监管部门、网络运营者数据活动的职责，对于维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全具有重要意义。

《办法》将弥补数据安全保护规则在部门规章层面的缺失，为数据安全领域的技术性规范和实践操作提供法律强制力，有利于行业规范体系的形成。它强化了监管部门的职责，可为数据的搜集和处理使用等营造良好的环境。《办法》可以有效遏制目前市场上普遍存在的盗用、滥用数据现象，为网络运营者提供一个公平、公开的竞争环境。《办法》明确了网信部门为个人信息和重要数据安全保护工作的主要监管部门，并对其监管职责进行了具体规定。正式实施之后，包括网信部门在内的监管部门可直接据此开展相关的监管工作。《办法》同时要求监管机关不能滥用网络运营者提供的数据，而应切实履行对数据的安全保护责任。

对于《数据安全管理办法》的发布，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、和谐的数据安全环境。

亿赛通签约中国石油天然气股份有限公司

客户简介

中国石油规划总院（CPPEI）是中国石油天然气股份有限公司直属的决策支持机构，是石油石化工程总体规划及建设项目前期研究中心、油气田开发地面建设技术支持服务中心和石油技术经济发展研究中心。在战略研究、规划可行性研究、咨询评估、技术经济研究、科技开发与设计论证等领域中，具有较强的技术实力。建院 20 多年来，CPPEI 已发展成为中国石油行业具有较高知名度的综合性咨询机构。

需求背景

中石油规划总院为国家一级涉密单位，在整体信息化安全建设方面先后已针对物理安全、网络安全、系统安全等做了相关建设并取得很好成效，但是在数据安全层面中石油规划总院仅仅在制度上进行了一定程度的制约，并没有通过技术手段去保护数据的安全，并且先后也出现过数据泄露事件。综上所述，中石油规划总院结合国家涉密单位的相关管理规定以及目前中石油规划总院的信息安全现状，最终决策采用亿赛通的文档加密系统保护中石油规划总院的数据安全。

解决方案

1. 驱动层加密：可对任意软件进行加密，并且在加解密效率上有明显优势；

2.AD 集成：可以与 CPPEI 现有 AD 域进行用户身份认证集成；

3. 流程化业务处理：系统所有业务处理均提供流程式的处理方式，符合中石油当前工作习惯；

4. 外发文件管理：在面向 CPPEI 外部的打印厂，可保障打印源文件的安全性。

项目成果

1. 所有涉密终端生产出的 MS OFFICE、PDF、AUTOCAD 图片格式文件均被强制加密；

2. 在中石油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须由本部门文档管理员解密，之后将文件拷贝至中石油涉密 U 盘中带出；

3. 中石油规划总院每天有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；

4. 中石油内网部署一套档案管理系统，用户经由该系统下载的文件只能自己查看，并且对于该文件只有只读、打印权限，同时该文档生命周期为 5 天，5 天后文件的使用权限自动销毁。

亿赛通签约中国石油化工股份有限公司

客户简介

中国石油化工集团公司（简称“中石化”）成立于 1998，是国家独资设立的国有公司、国家授权投资的机构和国家控股公司。公司注册资本 2316 亿元，主营业务范围包括实业投资及投资管理；石油、天然气的勘探、开采、储运（含管道运输）、销售和综合利用；煤炭生产、销售、储存、运输；石油炼制；石油化工、天然气化工、煤化工及其他化工产品的生产；中国石油化工集团公司在 2015 年《财富》世界 500 强企业中排名第 2 位。

典型案例 TYPICAL CASES

需求背景

随着中石化集团业务的急速发展，每天都会有大量的核心技术、专利、重要客户信息以及财务数据等方面的电子文档生成。虽然公司出台了安全相关的管理制度，但数据的应用过程中不管在服务器上还是在终端计算机上，都是处于明文存储状态，数据泄露的风险很大，中石化亟需加大数据安全投入管理。

解决方案

亿赛通文档安全管理系统帮助中石化具体实现如下功能：

1. 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；

2. 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；

3. 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；

4. 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；

5. 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；

6. 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。

项目成果

文档安全管理系统基于操作系统加密技术，文档加密过程不产生临时性明文文件，性能损耗低，支持超大型数据应用，单体文件最大可以支持 100G，从而助力中石化实现成本、效率、安全三者达到最优平衡。