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

9 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



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

4-8 国内行业新闻

9-15 国外行业新闻

亿赛通动态 ESAFENET NEWS

16/17 亿赛通出席新能源汽车智能制造专业论坛，安全攻防战悄然升级

18/19 徒步暴走 50 公里，亿赛通 & 绿盟科技助力公益为“爱”加油

亿赛通小贴士 ESAFENET PROMPT

20/21 台积电再生事端，内部员工盗窃核心机密，企业数据如何安防？

22/23 紧急公告！勒索病毒 GlobeImposter 出现变种 3.0

24/25 高校学生莫名其妙“被入职”，信息泄露到底有多疯狂？

26/27 网络电信诈骗让人防不胜防，这些“骗术”你都知道吗？

典型案例 TYPICAL CASES

28/29 亿赛通签约华晨宝马汽车有限公司

30/31 亿赛通签约广州本田汽车有限公司





喜迎双节，《亿赛通九月刊》新鲜出炉

秋风送爽，天高云淡，花果飘香，我们情系中秋喜迎国庆。在这个丰收与喜悦的日子里，亿赛通九月刊与大家共话信息安全大事，共建信息安全环境，共创未来安全。

汽车行业现今是民生之本，是制造业的典型产业。大数据飞速发展下，汽车制造业与智能化紧密结合逐渐成为发展的核心内容，是未来行业发展趋势，企业数据正在迅速膨胀并变大，成为易受攻击的行业与数据安全紧密连接。除了汽车行业，电子、半导体和高科技制造业更加容易受到威胁。台积电继勒索病毒之后，核心数据从内部流出，此次事件给领导者敲响了警钟，意识到数据安全的重要性。那么，为什么我们会频繁看到制造业发生的数据安全事件？本期月刊，亿赛通与大家共同诠析互联网、大数据与制造业企业数据究竟潜藏着哪些新威胁？数据安全行业解决新思路如何采取策略进行防护……

国内

1、新蛋网用户信用卡数据泄漏：恶意代码已侵入约 1 个月

摘要：北京时间 9 月 20 日，在过去约 1 个月的时间，购物网站新蛋 (Newegg) 的用户数据发生泄露事故，目前新蛋正在对网站进行整理。有安全研究人员发现，黑客将 15 行银行卡盗刷代码植入新蛋网支付页面，从 8 月 14 月 -9 月 18 日，代码一直存在。这种恶意代码从用户手中窃取信用卡数据，传输到由黑客控制的服务器。

2、最高法五年工作规划：拟出台相关司法解释，保护个人信息权



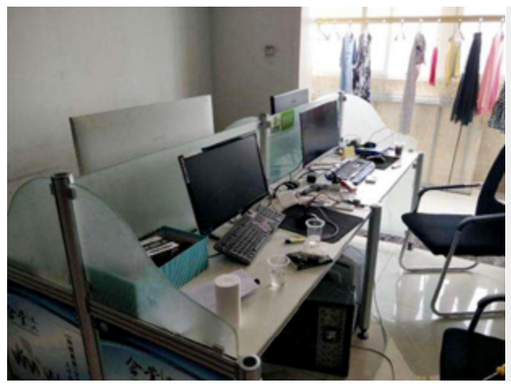
摘要：随着个人信息泄露事件的增多，人们对个人信息保护的需求也不断高涨。近日，最高人民法院发布《关于在司法解释中全面贯彻社会主义核心价值观的工作规划 (2018-2023)》(以下简称《规划》)。《规划》明确规定，要及时出台审理个人信息权纠纷案件适用法律问题的司法解释，保护个人信息权。

3、华住 5 亿信息泄露案嫌犯被抓 警方：用黑客手段窃取

摘要：上海警方抓获了窃取华住集团旗下酒店数据信息的犯罪嫌疑人刘某某（男，30 岁）。经查，犯罪嫌疑人利用黑客手段窃取华住集团旗下酒店数据，并在境外网站兜售，但未交易成功。

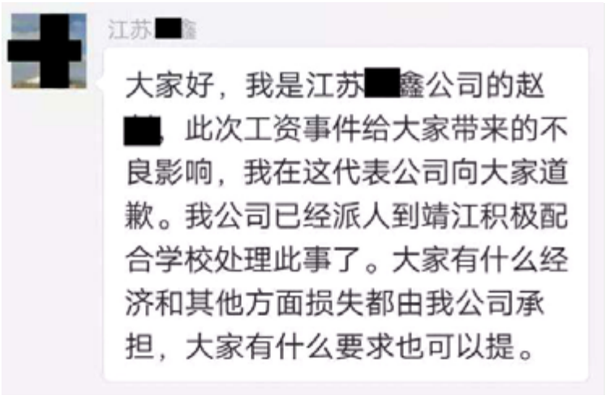


4、上百万公民信息泄露 温州警方摧毁“手持照”产业链



摘要：近年来，随着跨境电商业务的火爆，很多市民喜欢在境外购物平台买卖商品。这些网站不仅注册用户程序繁琐，还需要提供大量的个人信息，常常是一号难求。于是，一张小小的个人手持身份证照，竟被不法分子从几毛钱“炒”成几百上千元，卖给了大批注册用户。

5、江苏一高校 2000 多学生信息遭泄露 疑被企业用于偷逃税款



摘要：近日，有网友在社交媒体发布消息称，江苏常州大学怀德学院发生大规模学生信息泄露事件，上千名学生信息被不法企业盗用。记者调查发现，泄露信息的学生人数超过 2600 名，企业涉及省内多地，信息疑被企业用于偷逃税款。

6、买下 5000 元高档小区住户信息，结果他赚了 60 万



摘要：今年 5 月份，释某随公司来到建德设立了一个办事处，释某一心冲击业务，动足了脑筋，花了 5000 元买到当地一个高档小区 800 多住户的信息，有了这么详细的住户信息，他挨个上门或者电话，并且利用自己的经验“看人下菜”，竟然在短短 3 个月内，拉到该小区 60 多户的房屋装修业务，提成就达到 60 多万元，创造了公司在全国的记录，堪称“业界神话”。

7、青岛两护士售卖万余产妇信息获刑：2 元 / 条，流向早教等商家



摘要：近日，半岛记者从市北区检察院获悉，日前，市北区检察院通报了一起婴幼儿信息泄露案件，并完整披露了环环相扣的“信息生产销售链”，最终包括两名医护人员在内的六人犯侵犯公民个人信息罪，受到了法律的严惩。

8、350 余万条公民信息泄露 北京警方 4 天抓获 62 名嫌疑人



摘要：据北京警方通报称，为有效净化网络环境，打击网络侵犯公民个人信息违法犯罪，警方于日前对于前期掌握的网络侵犯公民个人信息违法犯罪线索开展集中收网行动。期间，北京警方共对 62 名犯罪嫌疑人采取刑事强制措施，查获各类公民个人信息 350 余万条。

9、顺丰 3 亿客户数据疑泄露 记者实测 20 条中 17 人为顺丰客户



摘要：近日，红星新闻接到爆料称，暗网中文论坛上有人出售顺丰快递与物流的相关数据，题为《顺丰 3 亿条快递物流独家数据》。从该爆料人提供的 10 万条验货数据中，红星新闻记者随机拨通十余人电话发现，电话、姓名和地址都是真实存在，电话主人也确实曾使用顺丰快递收寄物品。

10、今日头条前员工跳槽后留“后门”复活旧账户牟利涉罪

摘要：北京晨报讯 在公安部“净网 2018”专项行动统一部署下，海淀公安分局破获一起前员工跳槽后留后门，利用技术手段复活并倒卖废弃账号，非法牟利 200 余万元的黑客类案件，抓获犯罪嫌疑人一名。现嫌疑人罗某因涉嫌破坏计算机信息系统罪被刑事拘留。

国外

1、电脑零售商 NCIX 存了 10 多年的数据免费拿走，包括其创始人电脑备份



摘要：据外媒 ZDNet 报道称，一位安全研究员在 Craigslist 网站上发现了属于加拿大知名电脑零售商 NCIX 的客户和员工数据，且最早创建的数据可以追溯到 10 多年以前。

2、俄罗斯黑市 3000 多个网站访问权被出售



摘要：Flashpoint 的研究人员发布的一份新报告显示，在俄罗斯的黑市上可以访问超过 3,000 个遭受攻击的网站。最早的 MagBo 黑市广告于 3 月发布在一个顶级的俄罗斯黑客和恶意软件论坛上。根据广告内容，卖家提供的访问类型包括 PHP shell 访问、主机控制访问、域控制访问、文件传输协议（FTP）访问、SSH 访问、管理面板访问和数据库或结构化查询语言（SQL）访问。

3、 印媒：黑客利用印度网站疯狂“挖矿”，包括政府网站



摘要：一份由三名安全专家（Shakil Ahmed、Indrajeet Bhuyan 和 Anisha Sharma）组成的研究团队于近日公布的调查报告显示，包括安得拉邦市政管理局、蒂鲁帕蒂市政公司和马切尔拉市政机构在内的数百个印度网站都被发现感染了 Cryptojacking 恶意软件（又称“加密货币挖掘恶意软件”）。

4、 MongoDB 服务器配置不当！ Veeam（卫盟软件）4.45 亿条记录遭泄露



摘要：安全研究员 Bob Diachenko 于本周二（9 月 11）日发布消息称，由于配置不当，一个归属于 Veeam（卫盟软件）的 MongoDB 服务器暴露在了互联网上。该服务器包含了一个存储有 200GB 数据的数据库，然而它并没有受到密码保护。换句话来说，只要有人能发现该服务器，就能任意访问这些数据。

5、数千台 MikroTik 路由器沦为“矿工”，并主动将用户流量转发给黑客



摘要：近日，一场针对巴西人的大型加密货币挖掘恶意软件分发活动，主要受影响的是 MikroTik 路由器。结合各方报道来看，最终有超过 20 万台 MikroTik 路由器受到了感染，攻击者以此在巴西各地创建了一个庞大的 XMR 矿工僵尸网络。

6、美国国务院电子邮件系统遭遇入侵



摘要：美国国务院发言人透露，其非保密电子邮件系统遭遇入侵，部分员工的个人可识别信息面临泄露风险。这起入侵事件发生在美国国会议员批评其未达到联邦网络安全标准之后不久。美国国务院发言人表示，该机构正在跨部门，以及与私营部门服务提供商合作，以全面评估这起事件。

7、英国航空数据泄露：可疑代码现身



摘要： 网络安全公司 RiskIQ 称其发现注入英国航空公司网站的恶意代码，这些代码很可能是导致 38 万支付数据泄露的原因所在。RiskIQ 的研究人员声称，发现了抄录（skimming）脚本的证据，其旨在窃取在线支付表格的财务数据，在英国航空网站上发现的代码与攻击 Ticketmaster 网站的代码非常相似，但似乎这次攻击使用的代码根据英国航空网站的设计方式进行了特别的修改。

8、趋势科技多款人气安全应用程序被苹果下架，曝泄露用户数据



摘要：趋势科技开发的多个应用程序（包括 Dr. Antivirus、Dr. Cleaner、Dr. Unarchiver 等）因收集用户计算机的浏览历史和信息被苹果从其应用商店下架。被下架之前，这些应用都是人气应用，有数千条好评，评分介于 4.6 到 4.9 之间。

9、公民实验室：史上危险的手机间谍软件已感染 45 个国家 / 地区



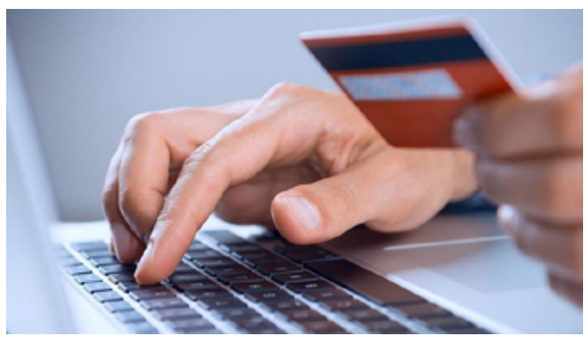
摘要：根据公民实验室（Citizen Lab）的一份最新报告显示，在过去的两年时间里，被认为是世界上最危险的手机间谍软件之一的 Pegasus 已经出现在了 45 个国家 / 地区，并被用于监控目标人物。Pegasus 可以说是 NSO group 最强大的创作，它被设计为能够远程攻击 iPhone、Android 和其他移动设备，允许攻击者访问一个目标受害者的大量数据，包括短信、日历条目、电子邮件、WhatsApp 消息、用户实时位置、麦克风和摄像头等。

10、Android 团队发现霍尼韦尔掌上电脑严重漏洞

摘要：谷歌的 Android 团队成员发现，霍尼韦尔的掌上电脑系统受到严重权限升级漏洞的影响。如果恶意应用程序进入受影响的设备，它可以允许其创建者提升系统权限并获取对敏感信息的访问权限，包括键盘记录，密码，照片，电子邮件和关键业务文档。



11、黑客组织 Cobalt 重新启用 CobInt 恶意软件，已向多家银行发起攻击



摘要：Cobalt 是一个至少在 2016 年就已经开始运营的黑客组织，主要攻击目标是金融机构。来自欧洲刑警组织的数据显示，该组织与全球至少 100 家银行的网络攻击活动有关，并从中窃取了超过 10 亿欧元。

12、儿童安全应用 MSpy 发生数据泄露，过百万被监控人信息遭曝光

摘要：MSpy 是一款帮助父母对孩子或合作伙伴的电话实施监控的软件，官方声称已有一百万付费用户选择了 MSpy。然而他们已经泄露了数百万条在线敏感记录，具体包括密码、通话记录、短信、联系人、笔记和位置数据等。

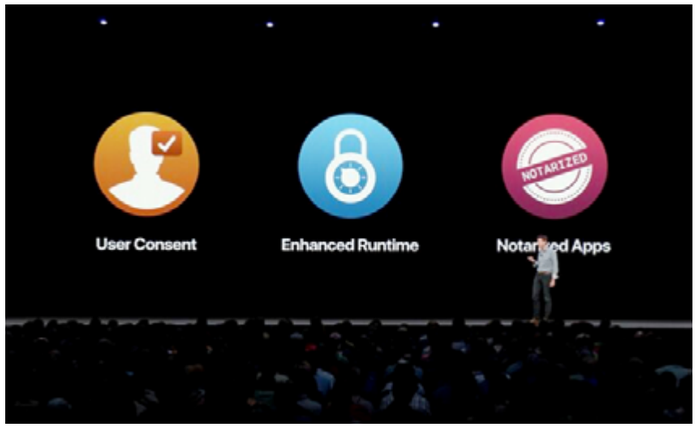


13、腾讯员工好奇检查酒店 WiFi 漏洞 被新加坡网警逮捕



摘要：在新加坡参加网络安全会议期间，一位腾讯工程师因为“好奇”入侵了其所住酒店的 WiFi，并将密码公布到博客上，结果被新加坡网络安全局逮捕，被罚款 5000 新加坡币。

14、刚发布就出问题 新 macOS 零日漏洞或导致用户数据泄露



摘要：苹果公司今天向全球用户推送了最新 macOS Mojave 系统。但是，一位安全研究人员称，新系统包含一个安全保护执行漏洞，可能会导致个人用户数据泄露。该漏洞会允许一款无特殊权限的应用绕过系统内建的系统级权限，获取特定应用的用户信息。瓦德里已披露了大量与苹果相关的安全问题，最近的一个是热门 Mac 应用 Adware Doctor 秘密记录用户信息。

亿赛通出席新能源汽车智能制造专业论坛，安全攻防战悄然升级



9 月 20 日，2018 新能源汽车智能制造专业论坛在上海举行，新能源汽车的智能化制造逐渐成为汽车制造业发展的核心内容，推进汽车工业的高端化发展，从整体上拉动社会经济的发展进步。新能源汽车制造是汽车工业发展的重要契机，为汽车制造的智能化提供了极为有利的条件。



新能源汽车与智能化紧密结合成为未来行业发展趋势，今年特斯拉再次被爆出内部员工泄露客户信息，车联网安全对攻战面临“二次发酵”。在新能源汽车制造业与数据安全紧密连接的市场现状下，会议邀请中国数据安全防护专家亿赛通为与会人员讲解汽车行业数据安全生态体系。

亿赛通公司技术专家在会上表示，“今天大多数已知的威胁和攻击都可以防御，但企业和机构面临更多的是未知的威胁和漏洞。主要的泄漏途径是内部人员泄密以及黑客、勒索软件攻击，所以传统的防御技术已经力不从心，需要通过智能技术的加密才能防御新的安全威胁。”

DATA IS MONEY

汽车行业无论是信息泄露的特斯拉、还是被破解的克莱斯勒，抑或是比亚迪秦，它们的共同点都是实现了高度的智能化。整个行业正在从传统的交通工具生产商向智能化、数字化服务商进行转型，其发展过程中的信息安全隐患使得提升信息安全水平、促进信息安全技术创新成为汽车行业数字化转型升级过程中关键性的一环。

亿赛通资深技术专家强调，目前大力推广智能化的新能源汽车领域，其数据安全隐患更大。“数据就是金钱”，现在最需要的就是一套完善的智能数据安全体系为车企数字化转型中技术、专利、图纸以及财务等核心数据的安全保驾护航。



亿赛通深耕国内数据防护市场多年，针对特定行业领域细分解决方案，逐步成为“敏感数据识别与主动防护相结合”、“终端 + 网络 + 应用”的全过程全范围数据防护服务提供商。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，实现“智能识别、智能分类、动态感知、智能加密、安全咨询”五大功能服务；针对核心数据存储、分级、管控进行“透明加密、权限管理、内容安全、外发管控、移动客户端、数据库审计、垃圾邮件网关”等主要产品功能，全面聚焦汽车产业链，构建安全生态系统。

公司在制造产业中先后为华晨宝马、佳通轮胎、哈电集团、海马汽车、广州本田、东风悦达起亚、长城汽车、中国北车、东风汽车电子等国内众多知名汽车企业提供数据安全解决方案。肩负着“保护数据所有者的信息资产安全”使命，不断进军国内外市场。

亿赛通总部在北京，同时在全国主要城市设有 30 余家分支机构，可提供全国性覆盖服务。未来，将以产品、方案、服务为主导，融合大数据和机器学习，构建包括终端数据防护、网络数据防护、应用数据防护、存储数据防护、介质数据防护和云服务平台在内的全范围智能数据泄露防护体系，全方位保障用户数据安全。

徒步暴走 50 公里，亿赛通 & 绿盟科技助力公益为“爱”加油



2018 年 9 月 8 日，

北京善行者公益之旅再次开启！

亿赛通 & 绿盟科技自发组建 11 支团队，

共同挑战徒步暴走 50 公里，

帮助贫困地区儿童健康成长！

恰逢善行者大型公益竞走活动五周年，

4 人一组，坚信“每一步都会带来改变”的信念，

体验行走的力量；

践行公益的承诺。



800 支队伍齐聚居庸关起点，

为孩子吃饱穿暖出发。

尽管初秋黎明的气温有些冻人，

但是依旧无法阻挡善行者们的热情。

感受宏伟长城



徒步传爱心



顺利完成挑战



此次善行，翻山越岭，

用行走的力量为那些需要帮助的人带来改变。

我们的每一步，

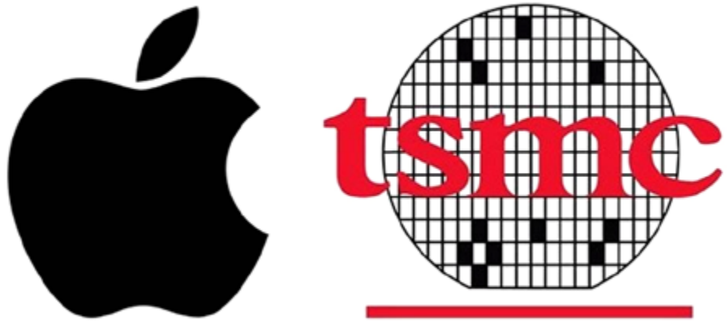
都承载着爱的希望，

为爱出发，为爱加油，

亿赛通将继续致力于公益事业，

传递爱的力量！

台积电再生事端，内部员工盗窃核心机密，企业数据如何安防？



内部员工窃取机密

说到产品保密，这大概是过去几年各大高技术公司最为头疼的事情了，作为智能手机领导者的苹果也不能幸免。苹果产品从产品设计、元器件采购、样品审核到产品组装整个产品线每一个环节都有可能成为其产品泄密的源头。日前，苹果A系列芯片的供应商台积电公司的一名员工被控从该公司窃取机密 ,并试图将这些机密带到新的公司 ,从而获得苹果的订单。

亿赛通小贴士 ESAFENET PROMPT



目前台湾新竹地区的检查机构已经受理了台积电的指控，据台湾当地媒体所披露的内容来看，该名员工为台积电任职 10 年的技术副理，其陆续将 16nm，10nm 等机密文件通过打印的方式保存，准备辞职。而台积电在清查的过程中发现了他打印机中的异样，对他发起了指控。

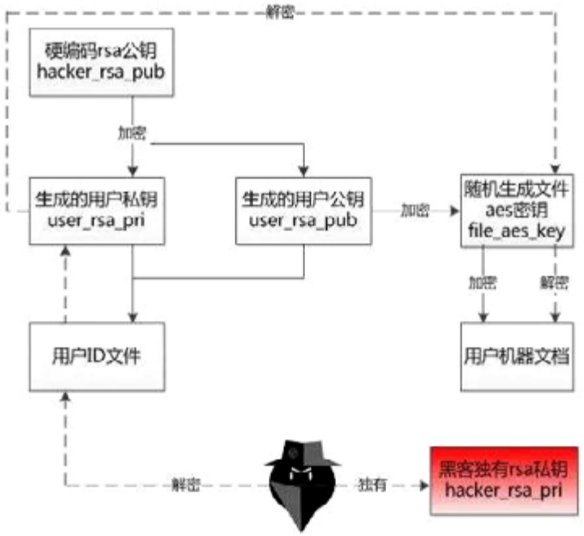
而这类事件，在苹果并不是个例，早在 2015 年，苹果公司就发生过有员工窃取公司机密，并向三星泄露获取利益，三星也的确因此受益，使其在芯片制造业务上迎头赶上。

常言道，外贼易防，家贼难防。在知识经济时代，市场竞争本质上就是知识产权的竞争，机密的泄露，很可能会关乎到整个公司的生死存亡。近些年关于高科技公司被窃密的新闻层出不穷，如何应对公司员工这种家贼式的商业间谍已经成为摆在各大科技巨头面前的一道巨大难题。

不过各位 BOSS 也请不要太揪心，亿赛通小贴士专家与您踏在一条战线，共同防家贼、消外患，全方位保障您的数据安全。亿赛通作为中国数据安全防护专家，15 年来一直致力于数据安全行业，其产品打响国内各个市场，广泛赢得客户的信赖，并与客户取得长期合作的关系，为其保障企业数据资产安全无风险。

亿赛通针对竞争对手窃密、员工离职拷贝、内部有意无意泄密、间谍 / 黑客窃密、设备丢失、非法脱机、电脑报废数据丢失、电脑拿到第三方去维修信息被窃等等的状况下，其所研发的产品以数据加密技术为核心，通过将技术平台与管理体系有效结合，可对任意文档自动透明加密，实现对用户核心数据资产的全方位保护。同时，通过信息安全边界的建立，降低核心数据资产如源代码、设计图纸、财务数据、经营分析以及其他任意信息资产有意或无意泄密风险。此外，配合完善的信息安全咨询服务，对企业的业务进行梳理和流程建立，保障企业的核心业务正常运转。

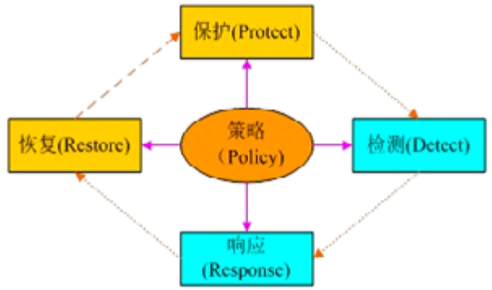
紧急公告！勒索病毒 GlobeImposter 出现变种 3.0



八月至今国内多家大型企业遭遇 GlobeImposter3.0 变种勒索病毒侵害，并呈现爆发的趋势。黑客通过入侵企业内网利用 RDP/SMB 暴力破解在内网扩散，投放 GlobeImposter3.0 勒索病毒，在进入内网后 通过多种方法获取登录凭证并在内网横渗透传播，此次爆发的勒索病毒并不区分被入侵机器是否有服务器，一旦入侵成功后，所有文件都被加密后辍名为“WALKER”的文件。

GlobeImposter 勒索病毒首次出现发生在 2017 年 5 月，第二次出现在 2017 年 11 月。GlobeImposter2.0 勒索病毒在今年 2 月份被发现，随后 8 月再次爆发。

由于 GlobeImposter3.0 采用 RSA+AES 算法加密，文件被加密后会被加上 Ox4444 后缀。在被加密的目录下会生成一个名为”HOW_TO_BACK_FILES.txt”的 txt 文件，显示受害者的个人 ID 序列号以及黑客的联系方式等。



1．该病毒在被感染系统中生成如下自身拷贝文件 :%AppDataLocal%\{Malware Name}.exe

2．在系统目录中生成如下文件 :

%SystemRoot\Users\Public\B26A340109A0081ADF57D63647533B8681DC0B8E159BE052385ED4024E9CFFBC

3．为达到自启动目的 ,该病毒添加如下注册表键值 :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce BrowserUpdateCheck = %Application Data%\{Malware name}.exe

4．被加密后的文件扩展名为 :ALCO

5．其会在加密文件路径下，生成如下勒索提示信息文件 :how_to_back_files.html

6．生成的勒索提示文件，主要包括受害者个人的 ID 序列号和勒索者的联系方式

解决方案

勒索病毒一旦中招必将损失惨重，因此积极防御就显得尤为重要，而防范勒索病毒的终极手段，还是要从源头对数据资产进行保护，坚决不给勒索病毒以可乘之机。

亿赛通勒索病毒防护卫士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。

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。

您可以通过以下方式联系我们，获取关于勒索病毒防护卫士的详情及支持服务：

1）拨打服务热线 400-898-1617；

2）PC 端访问亿赛通官网 www.esafenet.com，选择右侧 QQ 客服，进行在线咨询。

高校学生莫名其妙“被入职”，信息泄露到底有多疯狂？



热议话题＃江苏高校上千名毕业生“被入职”

又是一年开学季，不少准毕业生为找工作忙的是焦头烂额，发出了毕业即失业的感叹。然而江苏常州大学怀德学院的学生却恰恰相反，没有找到工作的他们却发现自己“被入职”了。

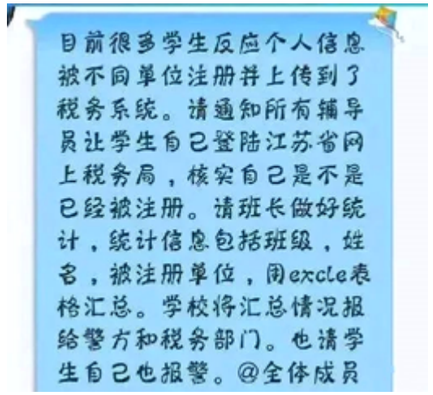
近日，有网友在社交媒体发布消息称，江苏常州大学怀德学院发生大规模学生信息泄露事件，上千名学生信息被不法企业盗用。

事件　信息泄露谁该承担责任？

王某是常州大学怀德学院 2018 届毕业生。9 月初，他在江苏省网上税务局查看税务信息时发现，至今没有找到工作的他，竟然在一家企业“上了班”，还交了税。之后与同学沟通发现，很多同学都存在这种情况。在没听过的企业申报了月薪并交了税。不仅仅是应届毕业生，不少大四的学生信息都被不法企业获取虚开工资。

校方在学生反映后，相关部门负责人立即和几名信息被盗用的学生一起去派出所报警。经核实，已有 2600 多名学生的信息被泄露，占在校生人数的三分之一。

盗用信息的企业负责人之一表示，学生信息并非购买获得，但具体来源拒绝回答。他可以肯定的是，企业没有雇佣黑客入侵高校系统获取信息，由此看来，学生信息是从学校内部流出。



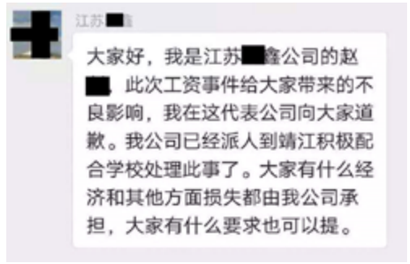
小贴士 多地存在学生“被入职”情况

常州大学怀德学院的信息泄露事件并非首例。2017 年，南京理工大学泰州科技学院也出现过类似爆料，学生反映江苏某保险代理公司盗用了他们的个人信息，疑似用来偷税漏税。在微博、微信等社交平台内，还有江苏无锡、云南昆明等地的学生均透露有类似遭遇。

此次，企业负责人向大众承认，用学生信息抵扣用工成本，为了年底少缴税；购买信息是犯法的，所以这些学生信息肯定不是买来的。

在此，小编向各位 boss 普及一点小知识：通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

因此，不管企业是否存在信息买卖行为，在学生不知情的背景下利用其信息虚列工资，已经涉嫌非法提供和获取公民个人信息，涉嫌犯有侵犯公民个人信息罪。



技术绝招：药到病除 构建校园内部信息安全管理体系

对于盗用学生信息企图偷税漏税的情况，相关部门都快速地作出了反应，但措施大都局限在“事后”解决上。所以，从学校方面就必须要从源头消除类似事件发生，要将安全意识和技术手段结合起来共同保护学生个人信息。国内一家知名的数据安全防护专家亿赛通，与众多重要行业携手打造客户信息安全，既保证企业业务较高的可用性、可靠性、保密性，又对内部核心数据有较强的防御、管控能力，如电子文档安全管理系统，实现了企业内部电子文件的加密存储。无论是由人工生产还是由应用系统生成的，只要写在磁盘上就是加密形式，倘若未经合法许可将加密文件数据体被带走，加密文件内容将不能够被正常打开，从而确保文件内容不会因为文件数据扩散而泄密。

亿赛通数据安全管理体系可以有效支撑高校信息管理业务，提升校园内部信息安全工作的发现、管理能力与处理效率，为教育行业安全贡献重要技术力量。保护隐私信息安全，亿赛通从不懈怠，一直做好中国数据安全防护专家。

网络电信诈骗让人防不胜防，这些“骗术”你都知道吗？



近年来，网络诈骗的案件高发，骗子们网络世界中变换各种角色，运用各种谎言伪装自己的身份，诱使受害人上当受骗。甚至，有的受害人被骗的倾家荡产，最终失去了自己的生命……

山东临沂的大学生宋某遇到电信诈骗，被骗去数额不等的现金后，心脏骤停，不幸离世！作为家中独子，父母受不了打击，整日精神恍惚，最终住进医院。一次诈骗摧毁了一个家庭！

除了宋某，还有很多血的教训，今天，小编跟大家一起来分享实际案例，遇到类似情形时，一定要采取正当的途径。千万提高警惕！

“官方”的客服

前段时间，济南的王女士碰到这么一件闹心事儿，她的微信号码忘记了登录密码，更换了手机号码，无法登录。微信余额里钱还没取出，于是王女士便想通过客服找回密码，然而王女士等了一段时间也没有接到反馈。这时，心急的王女士便从网上搜寻客服其他联系方式。别说，还真的搜到了一个“官方”的客服电话，而且这个电话一打就通了。

对方向王女士了解了一下具体情况，当即表示可以帮助其解决问题，只需提供一下现在使用的手机号，银行卡号等。同时，对方还询问了王女士的银行卡余额，表示只有银行卡余额大于微信余额时才能办理业务。王女士对网络并不熟悉，对所谓办理过程更是一知半解，只听到可以找回自己的钱便一步一步地根据“客服”的要求操作，告知了对方银行卡号、余额，还按照对方的要求输入了验证码。 谁知验证码一输入，业务没有办成，原本银行卡里的钱也被划走了！

网上的“警察”

“ 网上可以报警吗？有人利用网络骗钱，我被骗了，我有他微信、QQ、聊天记录什么的，可以网上报警吗？” " 网上被骗，报案加（q）XXXXXXXX" 除了在网上搜索客服的，还有受害人在网上被骗后，直接搜索“网络警察”报警，结果警没报成，再次被骗。

随着网络的发展，在网上搜索各种信息已经成了一种习惯，而也是这种习惯让犯罪分子钻了空子。其实，现在很多网站已经贴出了预警信息，只要你能平复心情，多加留意，就能避免上当受骗。



近期发生的网络电信诈骗事件很多，常用“套路”如下：

面对面将钱骗走

济南火车站，一名谎称在校大学生的男青年，以钱包丢失为由向过往旅客借现金，然后用支付宝转账还钱。想想大家出门在外，谁都有遇到难事的时候，所以旅客张某取出 700 元现金给了男青年，骗子向张某出示了一张支付宝还款的截图，然后说火车站信号不好，大概俩小时才能到账。张某看截图上有自己的账号，觉得挺靠谱，因为急着赶火车就走了！没想到就这么被骗走了……



“套路”分析

实际上，这仅仅是一个支付宝的待付款页面中间的一部分 ,页面上方还有个“等待付款”,下方还有个“立即付款”，但骗子拉大了整个页面，只让受害人看到了中间的截图。

温馨提示：支付宝账户转账即时到账 ,不存在 “延时”现象！

微信付款码诈骗

不久前，杨女士看到自己的微信朋友圈有人在集赞送奖品，想也没想就转发到朋友圈求赞了。没几个小时，这条朋友圈点赞量就上百。之后，她通过扫二维码加了转发信息里的那个叫“欣欣儿童玩具商城”的好友，对方说需要她提供微信钱包里的付款二维码的截图，好核实有没有重复领取，并申明，不需要杨女士付款，只要截图。

就这样，杨女士给对方发了三次截图后，对方还是说失效，并让她再次发送付款二维码。就在这时，杨女士手机连续收到了三张微信支付凭证，每一笔的付款金额都是 999 元，合计 2997 元。



“套路”分析

微信付款码不能随便给别人，网络中索要付款码截图的都是骗子！

“剁手党”最新套路

杨某收到一名“快递员”的电话，对方说她的收件地址字迹模糊，特意打电话询问地址，杨某就把地址告诉了对方。收到快递后，她就接到一个电话，对方称是中通快递总部，快递员送错了地址，请快递员接听电话。此时，刚离开的“快递员”又匆匆赶了回来，说自己手机没信号，想借手机给总部打个电话。男子接完电话告诉杨某，快递没弄错，随后归还手机离开。此时杨某才发现手机上收到了两条短信：一条是银行客服发来的转账验证码，一条是被转走 34500 元的提示。

“套路”分析

网购送货快递员的电话可以在网上直接查到，出现上面的情况，可以通过官方购物网站或者快递官方客服进行沟通，其他短信电话发的信息一概不要理会！

亿赛通小贴士再次提醒大家，所有信息都只能相信官方网站、官方渠道，不要轻信不明网址，不要添加未经验证的 QQ、微信号码。遭遇电信网络诈骗，及时拨打 110 或到当地公安机关报警！

亿赛通签约华晨宝马汽车有限公司



客户简介

华晨宝马汽车有限公司成立于 2003 年 5 月，是宝马集团和华晨汽车集团控股有限公司共同设立的合资企业，业务涵盖 BMW 品牌汽车的生产、销售和售后服务，公司的销售和服务网络遍及全国，成为中国最成功的高档汽车制造商，引领中国高档车市场的发展。

需求背景

由于公司的销售和服务网络遍及全国，华晨宝马需要与各个业务发展区域进行信息往来，加之企业内部人员流动性较强，数据易被拷贝、携带，以及竞争对手易窃取敏感信息，公司高度重视数据管理。

解决方案

亿赛通移动终端管理系统主要为防止利用移动设备非法获取应用系统数据的智能终端安全防护系统。移动端数据防护系统主要通过移动端用户身份认证、移动终端数据存储于访问控制等手段，实现对移动终端的数据使用安全控制。

统一身份认证：完善的统一用户身份认证管理体系，支持 Ldap 和 OpenLdap 的集成；

数据安全传输：数据始终以密文形式传输、存储和使用，保障传输过程中的安全；

终端数据加密：移动终端采用底层动态加密解密核心技术，保障落地数据安全；

系统安全集成：可与既有内网应用系统无缝集成，全程透明，不改变用户操作习惯；

终端自我保护：全球首创 Anti-hacking 技术，防止移动终端应用程序被反编译或破解。

项目成果

亿赛通移动终端管理系统使得华晨宝马公司的应用系统下载文档后被动态加密，终端动态解密审阅落地安全文档。灵活的部署系统不改变用户网络结构和客户的使用习惯，保障了每一个输入、输出的数据安全运行。

亿赛通签约广州本田汽车有限公司



客户简介

广州本田汽车有限公司成立于 1998 年是由广州汽车集团公司、本田技研工业株式会社和本田技研工业（中国）投资有限公司按共同投资建设和经营的企业，占地总面积为 393 万平方米，年产能力为 60 万辆。2016 年，广汽本田迎来了 Honda、理念和 Acura（讴歌）三品牌运营的新阶段，三大产品品牌并驾齐驱，形成完整的品牌矩阵，满足中国消费者日益多样化的产品需求。

需求背景

由于广州本田在不断满足市场需求现状和激烈竞争的市场环境下，企业业务需求的驱动、管理部门的驱动，如何有效实现企业重要信息系统的敏感数据安全管控成为广州本田的首要目标。

解决方案

亿赛通全盘加密安全 U 盘是公司自主研发，是国内最专业的基于物理磁盘全盘加密技术（FDE）的安全 U 盘。并通过硬件控制方式对 U 盘存储区域进行保护，杜绝暴力破解或底层非法入侵。

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

广州本田选择亿赛通全盘加密安全 U 盘产品，无论从专业角度还是产品的安全角度都具有强有力的竞争优势，产品依托国密芯片搭载亿赛通核心加密技术，从而保障广州本田内部重要数据在全盘加密安全 U 盘使用中实现零空间存储，保障财务数据、各类报告、隐私数据、机密信息等对 U 盘数据进行全面安全保护。