数据安全研究

Data security research

2015 年第二期

2015 年 07 月 01 日

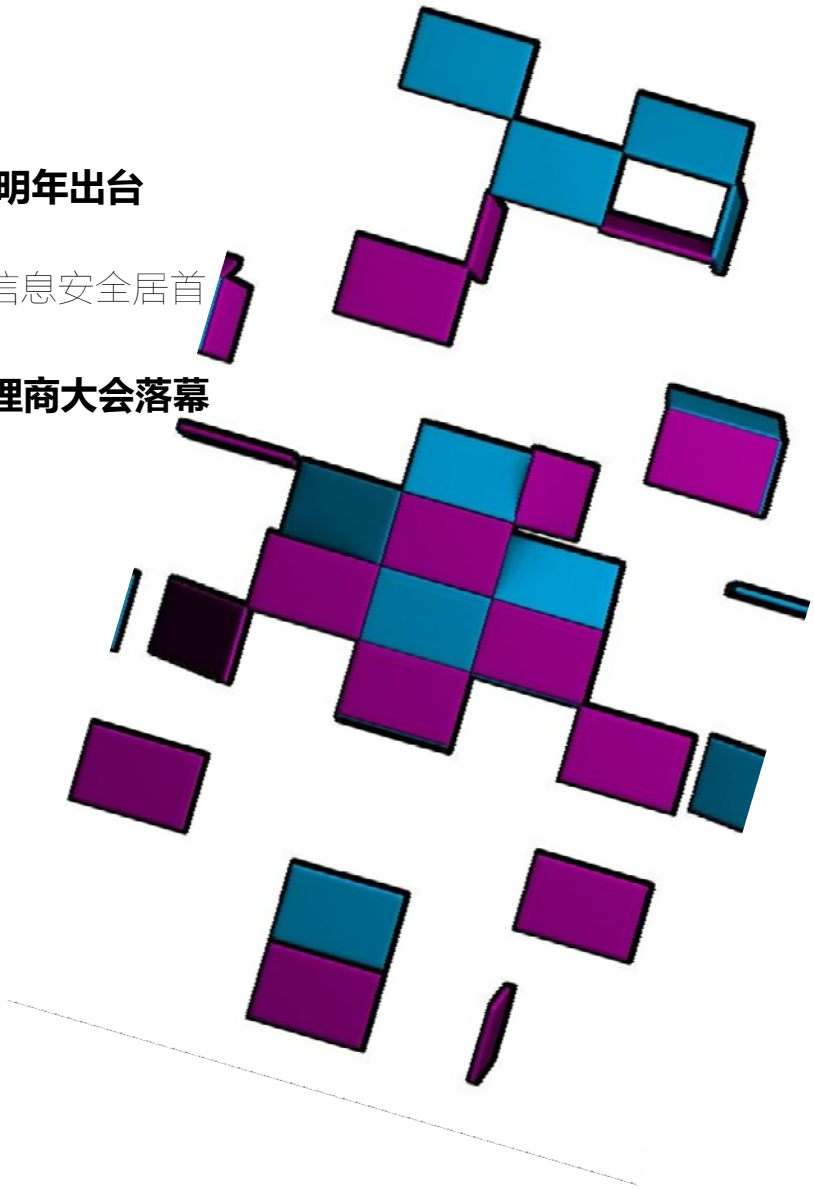
本期关注：

中国网络安全专项立法启动 最快明年出台

本科生就业满意度较高十专业：信息安全居首

合作创新 共赢未来 —效率源代理商大会落幕

2015 年第一季度信息安全报告



Foreword

建 dang 节的手写祝福语

今天是党的生日，党命令我们：领导和团结周边各位老友，以终生幸福为目标，以终日快乐为目的，坚持哈哈大笑原则，坚持幸福生活，健康快乐，事事如意，为把人人变成幸福、快乐、开心的富裕人而奋斗！祝福七一建党节快乐！

Contents 目录

News 资讯

[本页资讯来源于网络]

2015 物联网技术应用 信息安全论坛南京举行

新华网南京 6 月 29 日电（徐婕）6 月 28 日，由国家互联网应急中心、江苏省通信管理局、中国通信学会物联网委员会等主办，江苏省物联网技术与应用协同创新中心信息安全分中心、南京邮电大学物联网国家大学科技园等单位承办的 2015 年物联网技术与应用 信息安全主题论坛在南京隆重举行。论坛围绕“互联网+”国家行动计划与物联网信息安全主题，加强物联网技术与应用的学术交流与产学研协同创新，为全国物联网领域的各行各业提供一个政策研讨、形势分析、成就展示、学术争鸣、技术交流以及协同合作的公共平台。

明朝万达王志海解读 C 轮融资：目标直指数据安全行业领头羊

明朝万达将拿出此次 C 轮融资的 2/3 投入到技术产品研发和服务体系上，加强技术创新，提高服务质量，提升用户满意度。同时，提升研发人员的福利待遇，未来还将推行股权激励，实现员工与企业共同成长。

国务院：加强网络和信息安全保护

国务院办公厅 7 月 1 日发布《关于运用大数据加强对市场主体服务和监管的若干意见》。意见明确，加大网络和信息安全技术研发和资金投入，建立健全信息安全保障体系。采取必要的管理和技术手段，切实保护国家信息安全以及公民、法人和其他组织信息安全。

2015 中国网络安全大会：瑞星虚拟化安全成焦点

2015 中国网络安全大会于 7 月 1 日在北京国家会议中心举行，瑞星携国内首款虚拟化安全产品——瑞星虚拟化系统安全软件及企业信息安全整体解决方案在展会上亮相。此外，瑞星公司虚拟化产品开发总监郑斌也受主办方邀请参加了本次大会，并在会上发表了题为《虚拟化系统环境下的安全防护》的主旨演讲，获得了与会嘉宾的一致好评。

实施“快递实名制”莫忘信息安全

推行“快递实名制”，能够对不法分子起到一定的威慑作用，有助于从源头上减少快递运输违禁品的几率，能够有效整治快递乱象，但同时也会给普通网购者带来个人信息泄露的隐患。因此，在推动实行“快递实名制”的同时，还需要更多配套制度，比如建立一套风险防控和信用管理系统，保护寄件人、收件人的个人隐私，给遵循“快递实名制”网购的人吃一颗“定心丸”，为快递运输加一把“安全锁”。

数据安全 新一代信息安全体系的核心

数据安全，新一代信息安全体系“核安全”

随着移动互联网、物联网、云计算和大数据等快速发展，数据安全正逐步引起并得到用户和企业的重视。同时，围绕核心数据资产的攻击、窃取、破坏等黑客行为日渐增多，黑客攻击令传统的应用安全、网络安全等“壳安全”措施越来越疲于应付。以保卫数据安全这个“核安全”为终极目标的“数据安全体系”正在成为新一代信息安全体系的核心，传统信息安全体系建设的重心正在向数据安全倾斜。

这种以数据安全为“核安全”，以网络安全、应用安全、物理安全、行为安全为“壳安全”的新的信息安全体系正成为信息安全行业发展的大趋势，这些改变将有利于在移动互联网、物联网、云计算和大数据背景下，解决传统信息安全体系难以处理的安全防护难题。

数据的“静态”和“动态”

在这里，我们先要阐述下数据状态这一个概念。

根据数据的生命周期状态，数据安全研究院将其抽象为“静态”和“动态”两种状态，其中“静态”是指数据未加密的原始状态，数据静态场景以存储状态为主；动态是指数据原始状态发生改变，可表现为加密、伪装、隐藏等，数据动态场景以传输为主。对应数据的生命周期，数据一共有四种状态组合：

静态数据的静态场景：产生后存储

静态数据的动态场景：产生后传输

动态数据的静态场景：数据加密、伪装、隐藏

动态数据的动态场景：数据加密、伪装、隐藏后的传输

数据安全，以不变应万变

除了瘫掉对方网络，黑客攻击的主要目的就是：偷窃或篡改有价值的数据。

作为普通用户和众多中小微企业，在信息安全保卫战里，没有雄厚的财力加强“壳安全”——“御敌于国门之外”，所选的信息安全策略只能是“以不变应万变”——首先保证核心数据资产的安全，用隐身术、伪装、加密、备份……以数据安全保障信息安全。

在这场保卫战里，数据加密技术、数据伪装技术是最好武器。

通过数据加密，即使黑客冲破外围的层层防护壳，拿到的也是一个从底层进了加密的数据。

通过数据伪装，让有价值数据隐藏起来，或成为无价值的数据冗余，黑客拿到也没有价值。

针对黑客的恶意删除或自己的误删，数据恢复技术、数据备份将是数据安全的又一道安全保险，其中，数据恢复技术是数据安全乃至信息安全的最后一道防线。

通过数据备份，删除篡改后可快速恢复，目前使用较多的是本地备份、异地灾备、云备份。

通过数据恢复，应对唯一的数据被恶意或误删除后，只要没有被覆盖掉，就可以迅速恢复。

数据安全，研究、标准将应运而起

2014 年 2 月 27 日，中央网络安全和信息化领导小组成立。这标志着中国信息安全受到政府前所未有的重视。

禁采 Win8、禁用赛门铁克数据防泄漏产品……政府和金融等领域信息安全监管标准等政策法规的相继出台，显示出中国在信息安全领域对自主可控的强烈诉求。

目前，针对数据、数据安全领域的学术研究、技术研发、标准制定也应运而起。

2015 年 6 月 12 日，全国首个省级“数据恢复重点实验室”在四川落成，在“数据恢复四川省重点实验室”挂牌启动上，来自数据安全领域的 15 位专家被聘请为重点实验室专家。实验室下设数据安全研究院、数据安全俱乐部，致力于数据安全领域的产品、技术研究与学术交流。

实验室主任梁效宁表示，实验室的建立，一方面能大力吸收社会资源，集中力量研究新一代信息安全新热点领域的新技术、新产品，探索数据恢复技术在这些领域的应用，填补行业空白；另一方面，

能快速打开发展通道，以科技创新为动力，进一步提高实验室在全国乃至全球信息安全行业的竞争力，实现实验室的科研成果、产品技术在国内领先、在国际具有一定影响力的目标。

数据安全，行业“台风”来

发轫于 21 世纪之初，经过近 10 年的发展，目前，中国的信息安全产业已经初具规模，已形成三大类、约二十小类、近百种产品的行业格局，防火墙、VPN、安全内容和威胁管理软件是最主要的产品种类。

在一过程中，中国的数据安全发展过于缓慢和滞后。数据恢复行业散、乱、差、无标准、无监管；数据加密没有自主核心技术；数据销毁还是空白；仅数据备份发展情况稍好，但也存在重视和投入不足。

近两年来，为顺应迅速崛起的信息安全市场强大需要，国内外信息安全市场硝烟四起，合众连横。纵观全球信息安全收购案例，数据安全俨然成为这场厮杀战中的被争夺的战略高地。

越来越多的传统信息安全厂商采取并购、联合的方式，弥补传统数据安全短板，快速补齐信息安全必要元素，形成完整的信息安全战略布局，从而搭建更完整的信息安全解决方案，打造市场竞争优势，并购后的企业在数据安全人才、技术、产品和客户等方面实现资源汇集。

2015，信息安全行业的整合还将继续。对于传统的数据安全行业而言，变革已经来临，DT 时代，对数据安全的强烈需求，吹生了数据安全行业的“台风”，台风中，只有那些掌握核心数据安全技术的猪，才能“好风凭借力”，直接上青云。

在更大的市场里，以数据安全为核心的信息安全防护体系之战，才刚刚拉开帷幕...

合作创新 共赢未来

——效率源代理商大会落幕

6 月 12 日，以“合作创新 共赢未来”为主题的效率源代理商大会圆满落幕，来自全国各省市的代理商、客户以及数据恢复相关领域的 15 位专家参加了本次会议。

大会主要介绍近年来效率源科技所取得的成就，包括省级企业技术中心认定、升级技术转移示范机构建立等，其中，最重要的是与内江师范学院联合申报的“数据恢复四川省重点实验室”正式启动。

另外，大会还对效率源全新研发的战略新品——DRS 数据恢复系统、可视化行踪轨迹核查系统、效率源数据安全中心软件等进行发布。

效率源在发展过程中，积极把握市场变革机遇，不断创新，不断推出新技术、新产品、新方案。为促进与代理商合作共赢的成果建设，效率源不断完善服务体系。一方面自建高精度生产线，专业稳定保障生产供应；另一方面制定完整的宣传材料、会展设计、解决方案等各环节营销支持；再者，建立培训、认证、升级、服务，全方位的售后维护体系，真正做到让合作伙伴在与效率源的合作过程中能够更安心、放心。

此次代理商大会圆满落幕，为效率源与代理商的强强合作打下了坚实的基础。正所谓“单丝不成线，独木不成林”，效率源期望与各位代理商建立深厚的友谊。新的合作，志在共赢！


2015效率源新产品发布暨代理商大会

中国网络安全专项立法启动 最快明年出台

随着互联网的普及，互联网安全成为全世界瞩目的焦点，这时针对网络安全的国家监管正在逐步加码。据悉，近期国家开始启动国家信息安全审查、关键基础设施保护和互联网信息服务等方面的专项立法，目前立法草案第一轮针对行业内的征求意见已经结束，按照计划最快有望明年出台，其中一项重要内容是下一步国家将有望建立重要网络设施安全保护制度并由国务院制定具体保护办法。

据了解，目前针对网络信息安全立法工作，国家有关部门已经召集了三大运营商和包括华为、阿里、腾讯、百度、360 在内的互联网巨头进行讨论和修改，下一步将会向公众征求意见。

值得注意的是，**构建完善的网络设施安全保护制度成为下一步战略布局的“重中之重”。**

一位业内权威专家透露，目前正在修订的网络信息安全立法内容将包括网络安全战略、规划和促进网络运行安全、网络安全监测预警与处理等多项内容，其中最为重要的一项是国家将对提供公共通信、广播电视传输等服务的基础信息网络，能源、交通、水利、金融等重要行业和供电、供水、医疗卫生等公共服务领域的重要信息系统，设区的市级以上国家机关政务网络，用户数量众多的网络服务提供者所有或者管理的重要网络设施，实行安全等级保护制度，重要设施安全等级保护办法将由国务院制定。

当前，信息安全“黑洞门”触目惊心，网站攻击与漏洞利用正在向批量化、规模化方向发展，用户隐私和权益遭到侵害，特别是一些重要数据甚至流向他国，信息安全威胁已经上升至国家安全层面。

据中国信息安全测评中心监测发现，2014 年 1 月至 10 月，全国网站被攻击次数达 38000 多次，截至 10 月，相关数据总体呈上升趋势。全国共发现恶意网站约 28 亿个。2014 年约有 200 多个政府网站存在严重安全隐患，多个政府网站遭黑客组织攻击篡改，由于被植入非法链接等，我国 300 多个政府网站发生安全事件。

补天漏洞平台数据显示，2014 年 5 月至 2015 年 5 月 27 日，能源领域出现漏洞总数 247 个，其中高危 196 个，信息可泄露漏洞达到 216 个。天眼实验室独立发现并监测到的情况显示，在命名为 APT-C-00 的 APT 攻击中，国内感染量 1047 个，从部委到研究所，再到下面的企业和院校全部被感染，覆盖全国 29 个省。

一位专家坦言，除了网站安全漏洞外，包括政府企业等掌握大量隐私信息、商业机

密、财产安全等数据的部门，因为缺乏有效监管和问责机制，导致其即使出现信息泄露问题，大多却置若罔闻，或者采取“捂盖子”的方法，只要不曝光就行。

“规范和立法显得更加迫切。”北京启明乐投资产管理公司董事长李坚表示。

美国斯诺登事件的发生，让全世界对于信息安全的重视程度达到了新高度，随着“互联网+”成为中国经济发展的新动力，信息传输和传播的安全性显得尤为重要。

国家信息技术安全研究中心专家曹岳表示，这些年我国信息化发展非常快，与此同时，相应的网络安全法律法规等存在滞后、错位等问题。在网络空间安全立法方面，核心部分是国家关键基础设施，特别是对关系国家安全和公共安全利益的系统使用的重要信息技术产品和服务实施信息安全审查制度，针对金融、能源、医疗、税收、财政等涉及重大公共利益的行业信息应当给予特别保护。他认为，一旦立法规范后，对于安全产业来说是利好，“产业碎片化”问题也会得到改善。

而随着信息安全上升到国家战略层面，信息安全产业也将面临发展“黄金期”。多位接受记者采访的分析人士认为，信息安全处于快速发展期，预计未来数年行业复合增速有望达 30%，政策面利好将进一步推动行业景气度上升。在此背景下，网络安全龙头企业有望成为资金下一风口。

据了解，除了谷歌自主研发安防产品，准备通过智能家居进军安防产业;阿里巴巴收购安全公司翰海源;百度收购安全宝补充自己的云防护体系;腾讯与启明星辰联手推出专门的企业安全产品等以外，360、腾讯、阿里等多个巨头也纷纷抢滩信息安全领域。

李坚认为，站在投资的角度上来看，计算机的硬件和软件行业都会明显受益。招商证券报告显示，在国家信息安全大趋势下，未来信息安全行业出现多家过 500 亿市值的公司基本无悬念，国际间信息安全军备竞赛升级有望推动板块估值切换。

本科生就业满意度较高十专业：信息安全居首

2015 高考成绩已经出来，各省查分已经开始，面对专业选择如何抉择，不妨看看本科生就业满意度较高的十专业，作为参考。本文为大家揭晓，望 2015 高考考生选报出适合自己的专业。

主要结论：

“信息安全”是本科毕业生就业满意度最高的专业；

“电力系统自动化技术”与“学前教育”是高职高专毕业生就业满意度最高的专业；

教育、医学相关专业的就业满意度虽高，但月收入不具优势；

并非学以致用，也可以找到理想工作。

基本发现：

“信息安全”是本科毕业生就业满意度最高的专业；

“电力系统自动化技术”与“学前教育”是高职高专毕业生就业满意度最高的专业；

从整体上看，“信息安全”是 2014 届本科毕业生就业满意度最高的专业，“电力系统自动化技术”与“学前教育”是高职高专毕业生就业满意度最高的专业。

具体来看，本科专业中，“信息安全”(75%)、“建筑学”(73%)、“小学教育”(70%)、“城市规划”(69%)、“新闻学”(68%)是就业满意度较高的前五位专业。高职高专专业中，“电力系统自动化技术”与“学前教育”(均为 69%)、“医学影像技术”(68%)、“石油化工生产技术”、“港口物流设备与自动控制”、“临床医学”(均为 67%)是就业满意度较高的前五位专业。

名词解释：

就业满意度：在被调查的毕业生中，由就业人群对自己目前的就业现状进行主观判断，选项有“很满意”“满意”“不满意”“很不满意”“无法评价”共五项。其中，选择“满意”或“很满意”的人属于对就业现状满意，选择“不满意”或“很不满意”的人属于对就业现状不满意。教育、医学相关专业的就业满意度虽高，但月收入不具优势从月收入角度看，2014 届本科和高职高专毕业生就业满意度较高的前十位专业，其毕业半年后月收入也普遍较高，但其中与教育、医学相关的专业在月收入方面并不具有优势。

具体来看，本科专业中，“信息安全”月收入最高，为 5026 元；“小学教育”“医学影像学”的满意度虽然相对较高，但收入并不具有优势，分别仅为 3292 元、3172 元。高职高专专业中，“石油化工生产技术”月收入最高，为 3717 元；“学前教育”“医学影像技术”“临床医学”“护理”“助产”“中药”的满意度虽然相对较高，但收入并不具有优势，分别仅为 2621 元、3148 元、2608 元、2643 元、2740 元、2674 元。

并非学以致用，也可以找到理想工作

从工作与专业相关度角度看，2014 届本科和高职高专毕业生就业满意度较高的前十位专业中，大部分专业毕业生能够“学以致用”。具体来看，本科专业中，“建筑学”与“医学影像学”(均为 97%)、“城市规划”(93%)工作与专业相关度相对较高；高职高专专业中，“临床医学”(98%)、“医学影像技术”(93%)、“护理”与“助产”(均为 92%)工作与专业相关度相对较高。

但也有部分就业满意度较高的专业在工作与专业相关度方面并不具有优势。如本科中的“播音与主持艺术”(51%)、“劳动与社会保障”(56%)专业；高职高专中的“港口物流设备与自动控制”(47%)、“石油化工生产技”(73%)专业。由此可见，并非“学以致用”也可以找到“幸福感”满满的理想工作。但这可能需要毕业生做出更多尝试，甚至放弃原专业领域积累的一些知识。针对这类

专业学生，高校需加强对他们的通识教育，通过在校期间的学习与锻炼，提高其个人综合素质和基本工作能力。

全国信息网络安全状况调查结果发布

16 日召开“2015 中国反病毒大会暨第十四次全国计算机病毒和移动终端病毒疫情调查发布会”上发布了国家计算机病毒应急处理中心最新完成的一份调查报告。结果显示：无论是传统 PC 还是移动终端，安全事件和病毒感染率都呈现出了上升的态势。

国家计算机病毒应急处理中心 2 月 2 日至 2 月 28 日组织开展了“第十四次全国信息网络安全状况暨计算机和移动终端病毒疫情调查活动”。

调查结果显示，2014 年，88.7%的被调查者发生过网络安全事件，与 2013 年相比增长了 37.5%；感染计算机病毒的比例为 63.7%，比 2013 年增长了 8.8%；移动终端的病毒感染比例为 31.5%，比 2013 年增长了 5.2%。

2014 年，对互联网影响重大的安全问题层出不穷，“心脏出血”（Heartbleed）漏洞影响了数以万计的服务器，敲诈者病毒、伪银行木马让上百万用户陷入困境，社交网络钓鱼真假难辨，网络安全状况日益严重，其中各种新型及变种的病毒、木马、恶意软件等发展趋势依然严峻。垃圾邮件的数量近两年也持续攀升，电子邮件成为主要针对性攻击的入口，这些攻击的目的仍是窃取用户的商业和私密信息并用以进行网络攻击及非法的网络行为，最终获取更高的经济利益。

2014 年钓鱼网站数量急速增加，调查显示 30.4%的用户遭遇过网络钓鱼 / 网络欺诈。攻击者通过制造恶意钓鱼地址诱骗用户点击，进而窃取访问者的个人敏感数据，网站仿冒成为网络安全的突出问题。网络欺诈形成了“网络 + 社交 + 电话”的复合模式。

2014 年网络犯罪黑色产业链开始在各国之间泛滥，俄罗斯、中国、巴西的网络犯罪分子通过地下论坛等多种途径购买定制的黑客工具，竞争日益激烈的地下黑市导致黑客工具的价格十分诱人；类似的网络犯罪集团还在美国和加拿大制造多起大型数据外泄事件。预计 2015 年越南、英国和印

度等国也将被黑客列为重点攻击目标，更多针对性来源和目标国家的名字，将会出现在 2015 年的盘点列表之上。国与国之间的通力合作，加大了共同打击网络犯罪的力度。

较之往年，2014 年漏洞数量大幅增加，随着微软在 2014 年终止了对 Windows XP 系统的服务，相继爆出了针对此系统的“零日”（0 - day）漏洞及其它诸多漏洞，同时利用漏洞的攻击也层出不穷，最典型的当属“心脏出血”（Heartbleed）漏洞和“破壳”（Shellshock）漏洞，它们的发现警示人们没有一个应用程序和操作系统是永不可摧的。

调查显示，移动互联网导致安全威胁叠加。2014 年，31.3%的用户遭遇过个人信息泄露，移动端受攻击的概率大大高于传统 PC 机。而大数据的发展降低削弱了个人信息的可控性，信息泄露事件频发。

手机支付类病毒呈现出一种融合化的发展动向。由于支付类病毒智能化程度提升，“仿冒”的银行 APP、电商、支付类 APP 散布在各大中小型的电子市场，一旦点击下载，就会触发进入黑客操控的支付流程。手机支付类病毒正走向高危化、智能化，融合社会工程学等多种特征的发展趋势。

面对网络安全的严峻形势以及网络犯罪活动频发与升级，我国加速了信息安全法律法规的制定，同时也加大了对网络犯罪的打击力度，各部委联合组织了“净网 2014”、“剑网 2014”等专项行动全面治理网络乱象，打击网络非法行为，净化网络环境；加强了国际合作。同时，十八届三中全会上也提出了“依法治网”的概念，标志着我国已全面深入地进行网络安全法制建设。

2014 年国内外数据泄密事件回顾

Verizon 发布了《2014 年度数据泄露调查报告》，报告中回顾了 63737 起赛博安全事件和 1367 起已经确认的数据泄漏事件。报告数据显示：由于数据库原因产生的信息泄漏高达 25%。盘点 2014 年发生在国内外的数据泄密事件，探寻其背后的深层技术原因。实际上还有许多泄密事件，或正在调查，或无从确认，或无法公开。

2014 年国内外都发生了哪些信息泄漏事件？这些事件的背后的深层技术原因是什么？且听且分析：

春运第一天 12306 爆用户信息泄露漏洞

支付宝前员工贩卖 20G 用户资料 一条可卖数十元

2000 万开房信息泄露案开庭

小米陷“泄密”门 业内称违法成本低是根源

棱镜门事件再发酵

软件商“侵”车管所系统“删违”万余条

国内 130 万考研用户信息遭泄漏 正被黑产利用

韩 2000 万信用卡信息泄露 引发“销户潮”

通过 2014 年 Verizon 数据泄漏调查报告和全年的数据安全事件，可以发现以下几种数据泄漏原因：

以上事件，不难发现，大多数企业的安全管理和防护都无法跟上网络犯罪的脚步，入侵只需要数分钟或数小时，而企业发现和识别攻击则需要数周甚至数月。

使用失窃账户密码依然是非法获取信息的最主要途径，三分之二的数据泄露都与漏洞或失窃密码有关，这进一步凸显了两步认证的必要性。

虽然外部攻击远超过内部攻击，但是内部攻击有抬头趋势，尤其是与知识产权有关的内部攻击。

总体来讲，Version 报告发现病毒是第二重要的赛博安全事件，占 20%，紧随其后的是内部人员权限滥用（占 18%）和物理盗窃/损失（占 14%），在数据泄露中，对网页应用程序的攻击导致了35%的数据泄露。

内部人员的滥用数据库存储的有价值信息导致数据资产丢失。

安华金和安全研究人员建议从以下几点措施来实现数据的安全防护：

措施一：保护核心数据安全，建议使用数据库风险评估工具，定期对数据库进行安全风险检查，发现数据库使用中的安全隐患，及时人工进行加固；

措施二：安全管理员要了解本单位数据库中的敏感信息，采取有针对性的安全防御措施，对数据库中的敏感字段进行加密存储，即使整库丢失也不会泄密；

措施三：通过网络上的虚拟补丁技术对数据库漏洞的攻击特征进行识别，及时拦截来自外网的黑客数据库攻击；

措施四：运维人员对数据库中的敏感数据修改，一定要记入审计记录，如果出现非法篡改行为可以通过事后追责定责；

措施五：对从数据库批量导出数据的行为、整表删除、不带条件的更新等恶意行为及时中断数据库操作，防止数据库非法操作行为的发生；

措施六：在应用系统上线前，要对应用和数据库进行安全风险评估测试，及时发现并修复存在的安全隐患，如：SQL 注入点、后门程序、缓冲区溢出漏洞等。

2015 年第一季度信息安全报告

近日，趋势科技发表了最新的“2015 年第一季度信息安全报告”，报告指出医疗产业、iOS 设备与 PoS(销售终端)为新兴恶意攻击目标，大型攻击事件频传，2015 年第一季度就有近一亿美国人的医疗个人信息遭外泄。同时，2015 年恶意威胁数量也再创新高，第一季度平均每月拦截到的恶意威胁数量高达 47 亿，较去年同期增加 15 亿， 移动恶意 APP 数量在第一季度更是突破 500 万大关！无论是政府机关、企业或个人，都应提升信息安全防护意识，以降低遭受黑客攻击的机会。

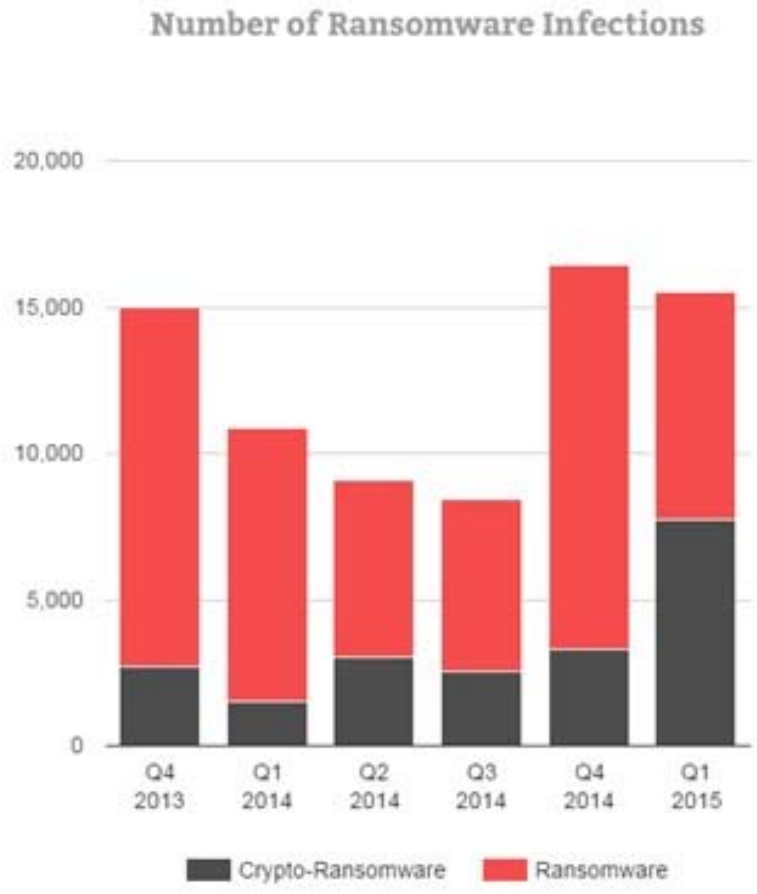
移动安全威胁突破 500 万大关

伴随着移动设备的盛行，移动设备恶意威胁的成长幅度以惊人速度大幅攀升，已于 2015 年第一季度突破 500 万大关。趋势科技信息安全团队发现，恶意广告是移动设备排名第一的信息安全威胁，今年三月份 Google Play 曾有超过 2000 个 App 可能含有恶意广告程序。此外，恶意网站也成为民众常误触的信息安全地雷之一，2015 年第一季度全球共有 800 万用户曾访问恶意网站。

随着移动应用更进一步的深入到消费者的生活之中，移动威胁将对数字生活带来更大的困扰。趋势科技已经发现不法分子利用恶意移动程序来骗取消费者信用卡的资金，由于很多消费者仍没有意识到移动设备存在的巨大风险性，移动安全威胁的增长趋势不会停止。

加密勒索软件侵入企业

2015 年，加密勒索软件 Ransomware 的数量还在不断上升。感染数量从 2014 年第一季度翻了两番，在 2015 年 Q1 到达了 7,844 个。在上一季度，加密勒索软件已经占据所有勒索软件将近一半（49%）的数量。



【勒索软件感染数量持续攀升】

趋势科技（中国区）技术总监蔡昇钦指出：“加密勒索软件 Ransomware 数量可能会继续上升。使用勒索软件是用恶意软件赚快钱的好方法。要建立一个殭尸网络、出租感染者、窃取银行凭证并从银行账户窃取资金将非常麻烦，勒索软件更直接。平均来说，每个勒索软可以拿到更多的钱。”

值得注意的是，加密后的办公文件被越来越多的被黑客用来勒索赎金。TorrentLocker 的模仿者 CryptoFortress 可以加密网络共享文件，同时，Ransomweb（CRYPWEB）可以加密网站和网页服务器，这些新发现的变种进一步确认了企业成为加密勒索软件的目标。

一种新的加密勒索软件 Ransomware CRYPAURA 可以加密超过百种文件类型。同时，Teslacrypt 会针对网络游戏玩家。通过“免费软件”模式来建立可信度，让网络犯罪份子可以诱骗玩家上钩。

加密勒索软件数量不断增加，并有扩大到企业的趋势，更应该加强个人和公司备份系统并确保文件受到保护。

第一季度信息安全报告的主要发现还包括：

·医疗产业遭受大量恶意攻击：大型医疗产业从业者，如美国阿拉斯加州最大保险公司 Premera Blue Cross 及美国大型医疗保险公司 Anthem 皆发生信息安全危机，超过 9100 万的客户金融及医疗数据外泄。

·旧信息安全威胁以新的攻击工具卷土重来。

·漏洞攻击持续增加新的攻击套件，越来越多网络犯罪专家及新手采用它们的攻击手法及技术。

·巨集病毒恶意攻击虽然老旧，但仍有效：于 2005 至 2008 年盛行的巨集病毒恶意攻击，目前仍在利用微软 Office 的系统漏洞进行恶意攻击行为。

·十年的 FREAK 漏洞带来补丁修复管理挑战：随著越来越多的安全漏洞出现在开源软件和应用程序，如何降低信息安全风险成为 IT 管理员一大挑战。

蔡昇钦表示：“虽然 2015 年才过去一半，但从大量、精细且复杂的恶意攻击手法来看，所有产业与组织皆无法避免恶意攻击，不论是企业还是个人都需要更积极及主动地部署信息安全防御，以对抗不断进化的多元型态信息安全攻击，以确保财产、个人信息及智慧财产权之安全。”

数据安全研究(半月刊)

每月 1 号，15 号定期相约

关于效率源

四川效率源信息安全技术有限责任公司是：

信息安全领域的创新者、数据安全行业的领军者

国家高新技术企业、双软认证企业、ISO9001 认证企业

知名数据恢复及司法取证设备的供应商

地址：中国四川省成都市高新区天府大道 1700 号新世纪环球中心 E3-E5 区 7 楼

电话：028-68731486；028-85055199

登录效率源官网：www.xlysoft.net

或效率源数据恢复论坛：bbs.xlysoft.net

微博搜索“四川效率源科技”关注我们，获取更多资讯和服务