耀騫說事

福泉南全

目录

前言

2011 年信息安全领域颇不平静，目标明确的新式攻击、黑客猖行、信息安全业界资本风起云涌、网络世界血雨腥风，数据丢失造成的损失惨重，如今攻与防的较量日趋白热化，网络已经成为一个新兴的战场。随着互联网和移动智能终端的快速发展，其开放性、共享性、移动性程度不断扩大，国际化、社会化和个人化的特点不断显现，在带给人们诸多便捷的同时也伴随着大量的安全隐患：有组织的网络犯罪日趋增多，利益驱动下的网络安全攻击层出不穷，针对特定国家和政府的敌对性攻击也开始出现。与此同时，随着电子商务和交易的迅猛增长，信息资源在经济、社会活动中的地位日益凸显，由此引发的盗用商业秘密和个人信息的现象屡见不鲜，给企业和市民的切身利益构成了威胁。

为了深刻揭示信息安全事件所带来的影响，更好应对信息安全风险，安言咨询汇编了相关媒体上发布的公开信息，以提名和投票的方式将过去一年中发生的重大信息安全事件做一个回顾，从中选出 22 件大事，编辑成《2011 年度重大信息安全事件回顾报告》。本报告将从危及国家安全类、重大社会影响类、重大经济损失类三方面，汇总介绍 2011 年度具有典型意义的重大信息安全事件，并对事件进行了初步分级。

危及国家安全类

典型危及国家安全的信息安全事件

本文收录了 6 个典型的危及国家安全类信息安全事件，包括伊朗核电站遭受攻击事件、RSA 遭黑客攻击事件、美中央情报局遭黑客攻击事件、日本三菱旗下军工企业遭黑客入侵事件、美国供水系统遭黑客破坏事件、美国安全情报智库遭黑客攻陷事件等。

危及国家安全类信息安全事件是指信息安全事件一旦发生，会对国家政治、军事、经济、文化、科技等造成严重威胁或危害。

本文事件的发生对象都属于能源、制造、运输、基础设施等行业工业控制系统，有的遭受了外部攻击，有的则是自身发生了故障，不论哪种情况，都将公众对信息安全的关注视线从传统的政府、金融、信息技术等行业转移到了以往公众乃至政府并不是特别重视的能源、运输等行业。

目前，工业自动化控制系统已经广泛应用于电力、水力、石化、钢铁、电器、医药、食品以及汽车、航天等工业领域，是国家关键基础设施的重要组成部分，在产品制造与服务提供乃至世界经济活动中起到了越来越重要的作用。工业基础设施构成了我国国民经济、现代社会以及国家安全的重要基础。然而，越来越多的工控信息安全事件的发生正在使我国的工业基础设施面临着前所未有的安全挑战。

工控信息安全不是一个单纯的技术问题，而是一个从意识培养开始，涉及到管理、流程、架构、技术和产品等各方面的系统工程。目前，部署纵深防御是工业领域应对安全挑战的现实方法，工控信息安全是一个动态过程，需要在整个工业基础设施生命周期的各个阶段中持续实施，不断改进。

目前，工业以太网和现场总线标准均为公开标准，熟悉工控系统的程序员开发针对性的恶意攻击代码并不存在很高的技术门槛。随着信息技术的不断进步，越来越多的民用技术正逐步运用到工业控制系统上，工业控制系统与一般金融企业、政府机构的信息系统的类似程度越来越高。而且由于网络的隔离和在线应用系统的重要性，出于系统整体稳定以及确保系统持续稳定运行的考虑，这些系统很少进行升级或采取必要的安全控制措施，一旦一点被突破，整个调度或在线系统将马上陷入危险当中。

在法律层面，针对工控系统也面临着严峻的信息安全形势，2011 年 9 月 29 日，工信部发布了《关于加强工业控制系统信息安全管理的通知》（工信部协[2011]451 号文，以下简称 451 号文），451 号文明确指出 2010 年开始的“震网”病毒对于工业控制系统信息安全的危害，同时要求加强对工业控制系统重点领域的信息安全管理。451 号文的出台，表明了政府对工业控制领域的重视，同时也为国内企业进一步加强工业控制系统信息安全管理提供了有效的依据和参照。

影响范围：★★★★☆
影响程度：★★★★☆
持续时间：★★☆☆☆

关键字：

伊朗 核电站 病毒 工业控制安全

伊朗核电站遭受计算机病毒攻击

事件回顾

Stuxnet 蠕虫（俗称“震网”、“双子”）在 2010 年曾攻击伊朗核设施电脑，2011 年伊朗国内网络又检测到与“Stuxnet”蠕虫类似的网络病毒。

2011 年 1 月 15 日《纽约时报》报道称，“Stuxnet”是美国和以色列情报官员在以色列绝密的迪莫纳核设施内联合研发的。该病毒在迪莫纳进行了两年的研发，随后被植入伊朗的核项目。这一行动被外界认为是世界上“最成功”的网络攻击。美国国务卿希拉里最近宣布，“Stuxnet”已使伊朗的核项目倒退了数年。

伊朗 2011 年 4 月称自己成为除“Stuxnet”外的第二种病毒的攻击目标，并将该病毒命名为“Stars”。伊朗 2011 年 11 月称已经检测到了被专家们认为是基于“超级工厂”病毒的“Duqu”计算机病毒。目前还不清楚“Stars”病毒与“Duqu”病毒是否存在联系，不过伊朗民防部门负责人贾拉利把“Duqu”病毒称为“意在攻击伊朗的第三种病毒”。

耀疆点评

1）信息攻击实现“自主精准打击”已经不是科幻情节。“Stuxnet”所展示的攻击效果，体现出高度的“精准打击”特性。它的传播机制、方法与常规病毒并无二致，但其发作机制却不同于常规病毒：它不是以窃取信息、破坏信息系统为目标，而是通过发出错误的离心机变频器运转指令来实现最终的破坏作用，更令人震惊的是：Stuxnet所破坏的工作参数在工业界中常出现在离心机等种类不多的设备中，而离心机正是核材料生产的关键设备，这充分体现了其“精准打击”的特性。

（2）信息攻击正在成为威胁国家安全的重大隐患乃至一种“武器”。“Stuxnet”利用了微软操作系统中的若干漏洞，其中包括3个未公开漏洞，它还成功地伪造了数字签名。这些都说明病毒的制造者具有强大的技术和人力资源保障。这一事件表明此类攻击已经可以作为一种武器威胁国家安全。

（3）现代信息攻击具备明确的目标，其策划和实施极具针对性。根据赛门铁克公司的统计，7月份，伊朗感染“Stuxnet”的主机只占25%，到9月下旬，这一比例达到60%。“Stuxnet”所攻击的WinCC系统被伊朗广泛应用于基础国防设施中。9月27日，伊朗国家通讯社向外界证实该国的第一座核电站“布什尔核电站”已经遭到攻击。据了解，该核电站原计划于2011年8月开始正式运行。而“Stuxnet”编写于3月，直到7月才大规模爆发，与这一计划不谋而合。因此，有充分的理由相信此次攻击具有明确的地域性和目的性。

（4）仅靠“物理隔离”已不足以抵御新型信息攻击。基于Windows-Intel平台及WinCC的工控PC和工业以太网，虽然与互联网隔离，但是仍然可能遭到攻击，例如可以通过U盘传播恶意代码和网络蠕虫，这次的“Stuxnet”爆发事件就是一个典型的例子。

中国在很多行业使用德国西门子、ABB或日本的SCADA系统或自动控制系统，如电力、钢铁、制造等行业，而且由于工控信息网络与互联网隔离，以及在线应用系统的重要性，很少进行升级或采取必要的安全控制措施，一旦一点被突破，整个调度或在线系统将马上陷入危险之中。建议逐步采用国产系统替代进口产品，以保障国家安全；过渡时期，也应尽量限制国外产品在关系国计民生的行业中使用；无论是否与互联网物理隔离，均应加强信息安全防护。

信息来源
中新网，
http://www.chinanews.com/gj/2011/11-15/3462140.shtml

影响范围：★★★☆☆
影响程度：★★★☆☆
持续时间：★★☆☆☆

关键字：

EMC RSA 安全厂商 密码被盗

著名安全厂商 RSA 遭黑客攻击事件

事件回顾

2011 年 3 月 7 日全球第六大企业软件公司 EMC(美国易安信公司)向美国证交会(SEC)提交报告称，公司下属知名安全厂商 RSA 遭遇黑客攻击，目前尚不知晓攻击涉及的范围，但可能令公司防黑客入侵技术的安全面临危险。报告指出，RSA 被一种业内称为“高持续性威胁”的复杂攻击手段入侵，这是一种“极其复杂”的攻击，会导致一些秘密信息从 RSA 的 SecurID 双因素认证产品中被提取出来。RSA 客户包括一些大军事机构、政府、各种银行及医疗和医保设备。

不过该公司表示，即使密码被盗，使用这些产品的电脑也不易被入侵。目前 RSA 正在与后端软件协作生成仅供设备用户知道的密码。

RSA 在报告中称,“那些被提取出来的信息不会对任何 RSA 的 SecurID 用户造成直接攻击，但这些信息可能作为更广泛攻击的一部分、被用来减少当前双因素认证实施的有效性。”

该公司执行董事阿特·卡威罗称，“目前尚无证据显示与其它 RSA 产品相关的用户安全受到该攻击的影响。另需指出的是，我们认为这次事件不会对客户及雇员个人确认信息构成威胁。”

耀疆点评

（1）安全永远都是相对的。对于黑客们来说，没有哪个目标是神圣不可侵犯的，连 RSA 这家世界上领先的安全公司也不例外。

（2）关键和基础安全产品的自身安全性影响是深远的，必须可控可信，厂商要承担相应的责任。RSA 遭到攻击后，最初该公司声称不会直接导致其SecureID产品的安全性丧失，但后来洛克希德马丁公司遭到攻击使 RSA 改变了立场，认可其遭攻击后泄漏的信息使攻击者得以破解 SecureID 的安全机制，最终导致洛克希德马丁公司被入侵。

信息来源
和瑞网，
http://stock.horise.com/news/20110318/00466022.shtml

影响范围：★★★☆☆
影响程度：★★★★☆
持续时间：★★★☆☆

关键字：

军工企业 服务器中毒 信息外泄

日本三菱旗下军工企业遭黑客入侵

事件回顾

2011 年 8 月 11 日，日本军工生产企业三菱重工旗下打造潜舰、生产导弹、以及制造核电站零组件等工厂的电脑网络遭到黑客攻击，并有资料可能外泄，这是日本国防产业首度成为黑客的攻击目标。

8 月中旬，三菱重工发现部分服务器中毒，邀请网络保安公司调查。他们在中毒的服务器和个人电脑中，优先分析存有核能、国防数据的服务器后，发现电脑系统信息外泄，服务器上的信息被胡乱移动的迹象，并可能有几个档案已经被窃。

网络保安公司指出，电脑可能在 8 月之前就已中毒，数据或早已长期被窃，目前正积极分析黑客入侵途径。三菱重工发表声明称，公司于 8 月 11 日发觉遭受网络攻击，一些系统数据如 IP 地址已外泄，但有关产品或科技的重要数据，至今仍然安全。

耀疆点评

信息安全是一个完整的体系，任何一个微小漏洞都可能导致严重后果。内部调查显示，这些电脑最早在 7 年前就已经被感染。据有关人士声称：据现在对已发现病毒的 83 台计算机依次分析所得出的结果显示，感染病毒的种类达到 50 种以上，比 9 月 19 日所发表的 8 种大幅增加。其中感染病毒最多的 1 台电脑上有 28 种病毒。在这些病毒之中，能窃取用户资料的蠕虫病毒“AGOBOT”早在 2004 年 4 月就已经被发现，并提醒注意。而能盗取银行帐号密码的“SPYEYE”也在 2011 年 7 月就得到过警告。

透过上述信息可以看出，早在此次遭受黑客攻击前三菱重工就已经发现了内部计算机感染了类似病毒，但之前的病毒感染事件显然未能引起三菱重工内部人员的足够重视，信息安全意识淡薄直接导致了本次黑客攻击事件的发生。

信息来源
中新网，
http://www.chinanews.com/gj/2011/09-20/3338635.shtml

影响范围：★★★☆☆
影响程度：★★☆☆☆
持续时间：★★★☆☆

关键字：

供水系统 基建设施 黑客破坏

美国供水系统遭黑客破坏

事件回顾

2011 年 11 月，美国一家网络安全监控机构提交报告，国外网络黑客几天前攻击美国一处地方水利系统。报告称，这是国外黑客首次瞄准美国工业设施网络监控系统实施攻击。

这份报告由伊利诺伊全州恐怖主义和情报中心提交，网络监控专家乔·魏斯 18 日向路透社记者披露报告内容。他说，黑客从一家软件公司获得授权信息，11 月 8 日侵入伊利诺伊州首府斯普林菲尔德以西的一处农村地区水利控制系统。实施攻击的电脑位于俄罗斯。

柯伦-格拉德纳镇公共水利部门律克雷文说，“攻击者利用一款远程监控水泵的软件系统，使一台水泵受损”。水利系统采用多水源和水泵系统，所以攻击没有造成供水中断。该供水机构覆盖当地 2200 家用户。

国土安全部发言人布高说，联邦调查局人员正在调查这件事。网络监控人员认为，攻击表明全美“监控和

数据采集系统”（SCADA）软件系统存在漏洞。这一系统控制诸多重要基础设施，包括水处理、化工厂、核反应堆、天然气管道、水坝和火车运行轨道控制系统。

耀疆点评

美国伊利诺伊州供水系统遭攻击后导致供水系统故障的事件再次唤起了公众对于工业控制信息安全的关注。传统意义上的黑客攻击往往针对金融机构、政府网站、知名企业等，但人们往往忽视了对于基建设施工业控制系统信息安全的关注与重视。

监控和数据采集系统”（SCADA）在美国国内影响广泛，该系统的稳定与否直接影响供电、供水、地铁运行等关系广大民众日常生活的各项活动。

此次美国供水系统遭攻击导致故障事件、伊朗核电站遭攻击导致异常事件再次引发人们基建设施（供水、供电、燃气等）尤其是涉及国计民生的工业控制安全的思考。这些事件同时也标志着黑客的攻击目标正在由金融、政府等传统攻击目标逐步扩大为更多与普通人日常生活密切相关的基建设施。

信息来源
网易新闻，
http://news.163.com/11/1120/15/7JAGVL9H00014AED.html

影响范围：★★★★☆
影响程度：★★★★★
持续时间：★★☆☆☆

关键字：

安全情报 黑客攻击 未加密

美国一安全情报智库遭黑客攻陷

事件回顾

12 月 26 日，在欧美非常活跃的黑客组织“无名氏”（Anonymous）声称，他们成功侵入美国知名安全情报智库“战略预测”的电脑，盗取了包括美国空军、陆军在内的 200GB 的客户电子邮件、信用卡资料等机密信息。

“无名氏”成员当天在社交网络上公布了被他们攻陷的“战略预测”智库的机密客户名单，其中包括美国陆军、空军和迈阿密警察局在内的重要机构。此次大规模泄密还涉及银行、执法机构、国防项目承包商和技术公司等，其中包括著名的高盛集团、苹果公司和微软公司。“无名氏”表示，他们能获取这些公司的信用卡资料，部分原因是该智库未对这些机密资料进行加密。若属实，对任何一个与安全情报有关的公司或智库而言都是一个重大尴尬。

该黑客组织一名成员宣称，他们将利用这些被盗取的信用卡资料，从中盗走一百万美元用于“圣诞捐款”。

该组织还表示，攻陷该智库只是他们为期一周的圣诞攻势的一长串目标的开始。

“战略预测”的创立者乔治·弗列德曼在发给客户的邮件中证实说：“我们有理由相信，我们的用户名单已经被公布到其他网站上，我们正在努力调查用户信息在何种程度上已经被黑客获取。”

弗列德曼还表示，用户的机密信息对他本人和“战略预测”而言非常重要，他将这次黑客攻击视为非常严重的事件，目前正在配合执法机构，调查究竟谁该为此事负责。

耀疆点评

“战略预测”是美国一家非常著名的民营智库，该机构是全球首屈一指的情报收集与预测公司，专门为各国政府和企业提供各类政经分析和预测，素有“影子中央情报局”之称。

黑客组织“无名氏”是一个松散的联合体，他们经常对一些政府和企业发动网络攻击，目前有关该组织的很多事情还是“谜”。早在 2011 年 8 月 6 日，该组织就曾宣称他们攻击了约 70 个美国执法机构的网站，其中大部分是地方一级执法机构。此次攻击再度验证了国际性黑客组织对于国家信息安全的重大危胁。

信息来源
新浪新闻，
http://news.sina.com.cn/w/2011-12-26/033423693594.shtml

影响范围：★★★☆☆
影响程度：★★★★☆
持续时间：★★☆☆☆

关键字：

中情局 黑客攻击 密码泄露 政府机

美国中央情报局遭受黑客攻击

事件回顾

2011 年 6 月黑客联盟 LulzSec 攻击美国中央情报局网站，黑客联盟 LulzSec 已在周三晚上宣布为美国中央情报局网站打不开负责。根据另外的报告，该黑客联盟还在上周四发布了 62000 个电子邮件账号和密码组合，并鼓励人们在 Facebook，Gmail 和 paypal 等网站上尝试这些账号和密码。之前，美国联邦调查局、参议院、任天堂、索尼、PBS、The Escapist 杂志、Eve Online、Minecraft、FinFisher 和 League of Legends 等著名机构都遭到了他们的攻击，黑客甚至还公布了一个电话来寻找攻击目标。

耀疆点评

在广大公众印象中，美国中央情报局作为世界范围内的知名情报机构往往笼罩着一层神秘的色彩，公众也往往相信中央情报局的网站和信息系统拥有超越一般政府和企业的安全性，但此次事件彻底颠覆了公众对于此类机构的安全印象，同时也再次印证了一个道理，世界上没有绝对安全的网站或信息系统。

信息来源
IDC E 网科技，
http://www.idcew.com/news/idcxinwen/4441.html

重大社会影响类

严重危及社会安全的信息安全事件

本文收录了 7 个具有典型意义的重大社会影响类信息安全事件，包括 PSN 平台用户数据泄露事件、美联合航空电脑故障致旅客滞留事件、韩国信息运营商信息外泄事件、多家国际证书机构遭到攻击事件、病毒侵袭智能工具 Android 系统事件、美移动运营商安装窥探用户隐私软件事件、CSDN 等多个网站用户信息泄露事件等。

重大社会影响类信息安全事件是指由于信息安全事件的发生对社会秩序、经济建设和公众利益等方面造成重大影响的信息安全事件。

当今世界是一个信息爆炸的时代，信息被看成是一种重要的战略资源，成为社会经济发展的重要因素之一。个人的数字化信息正在界定每个人的一切并成为其基本资产。但是，广大公众在访问网络论坛、社交网站、微博等新兴互联网网站时，并不会太在意网站的安全究竟做的怎么样。当发生了诸多涉及用户信息泄漏的事件后，广大互联网用户才开始真正关注互联网生活中的个人信息保护。

2011 年度涉及个人信息泄漏的重大信息安全事件再次给我们敲响了警钟。信息安全不仅是企业的事情，也是与每个人密切相关的。广大用户在使用网络应用程序时，应当事先了解该程序的用途以及其他用户对于该程序的评价，并注重个人信息的界定与保护。另一方面，作为在互联网上提供各类服务的互联网企业，更有必要加强对用户个人信息的保护，企业需要保护的不仅仅是用户通讯方式、地址等传统意义上的个人信息，对于用户口令，企业同样承担着不可推脱的责任。

值得人们关注的是，我国关于手机乃至移动互联网终端安全方面的法律法规目前仍是空白，个人信息保护法迟迟没有推出。据悉，国家有关部门正在加快制定信息安全相关标准与法规。建立健全信息安全法规，加大处罚力度对于保护信息安全至关重要，才能真正地进一步促进信息网络社会健康有序地发展。

影响范围：★★★★☆
影响程度：★★★★☆
持续时间：★★★☆☆

关键字：

索尼 7000 万 信息泄露 PSN

索尼公司 PSN 平台发生用户数据泄漏

事件回顾

2011 年 4 月 27 日，索尼公司承认其 PlayStation 网络平台（以下简称“PSN 平台”）遭到了黑客的入侵，导致超过 7000 万用户资料外泄。此事件不仅被载入用户信息泄露史，也让索尼领教了互联网以及移动互联网所带来的安全隐患。

索尼在其官方博客中发布了一份重要通知，提醒超过 7000 万的索尼 PSN 平台用户，他们的个人信息，包括姓名、家庭住址、电子邮件地址、生日、游戏平台 PSN 和云音乐服务的账户密码、用户名以及其他相关的网上信息都遭到了“匿名黑客”的盗取。据索尼提供的消息，这些数据在 4 月 17 日至 19 日之间遭到了非法访问。由于有不少用户向索尼提供了信用卡的相关信息，以便在平台上购买或租用相关游戏产品，所以这些信用卡账户面临被盗用的风险。

耀疆点评

事情的发展显然已经到了不受控制的地步。7700 万 PSN 网络用户资料的泄露，已经造成了世界历史上最大的信息泄露事件。黑客连接网络，通过破解网络服务器突破防火墙进入内网，访问应用服务器，破解应用服务器，通过应用服务器的漏洞注入通信工具，通过应用服务器破解数据库服务器，获取数据库服务器的权限，从存储设备上访问数据库数据，然后直接拿走用户资料。该次针对 PSN 的破解意味着索尼的网络，防火墙，网络服务器，应用服务器，数据服务器，数据库，以及存储硬件这一整套 PSN 系统的所有组成部分全部都已被破解，且这个数据传输不是一次性完成的，而是通过网络一点一点地慢慢地把索尼的数据盗走的，这也是为何这次 PSN 重建需要这么久的原因，所有的部分都要重新设定安全。

近年来，随着电子商务以及移动互联网的广泛应用，所带来的安全问题也日趋严峻。巨大的利益驱使黑客频频发动攻击，而用户的基本信息、网银账户、游戏账户密码等成为重灾区，这背后也形成了巨大的黑色产业链。

信息来源
搜狐，
http://business.sohu.com/20110428/n306616261.shtml

影响范围：★★★★☆
影响程度：★★★★☆
持续时间：★☆☆☆☆

关键字：

美联航 系统故障 航班飞机 上千旅客滞

美联合航空电脑故障致旅客滞留

事件回顾

2011 年 6 月 17 日晚间，美国联合航空公司的电脑系统出现故障，致使大批旅客滞留芝加哥市和丹佛市机场数小时。据悉，此次“崩溃”的系统包括航班离港、机场程序、预定系统、以及公司网页，自电脑系统出现故障至 18 日凌晨，大批旅客在机场值机柜台前排起长龙，上千旅客被迫滞留机场过夜，洛杉矶国际机场发言人表示，仅当地机场就造成 2500 人滞留。18 日凌晨 1 点左右，美联航在“推特”网上宣布故障已排除，电脑系统能够正常运转，这时距其电脑系统“崩溃”已经过去了 5 个多小时。芝加哥奥黑尔国际机场和丹佛国际机场是美国最繁忙的机场之一，本次事件造成了巨大的社会影响。

耀疆点评

公众对于信息系统安全的关注重点往往集中于政府、医疗、金融等领域，往往容易忽视航空公司的信息系统安全，但是此次美国联合航空公司信息系统故障再度唤起了人们对于交通运输领域信息系统安全的关注。值得注意的是，国外航空公司的信息系统大多采取“各自为政”的策略，正是由于这种策略使得该事件并未对美国国内其它航空公司的正常营运产生影响。

反观国内，与国外航空公司不同的是，国内航空业的票务预订、离港等业务均统一采用中国航空信息网络股份有限公司的计算机系统（简称“中航信系统”）。在确保各家航空公司统一协调、调度，提高工作效率的同时，也将所有风险都集中在了中航信系统之上。

通过此次美联航事件，有必要引起针对运输行业信息系统安全的关注，应当从业务连续性的角度出发，采取各类管理和技术手段，确保该系统的持续、稳定运行。

信息来源
搜狐，
http://news.sohu.com/20110618/n310635440.shtml

影响范围：★★★★☆
影响程度：★★★☆☆
持续时间：★☆☆☆☆

关键字：
新浪微博 病毒 私信

新浪微博病毒大范围传播

信息来源
凤凰网，
http://tech.ifeng.com/internet/detail_2011_06/28/7307936_0.shtml

事件回顾

2011 年 6 月 28 日新浪微博突然出现大范围“中毒”现象，多名用户账号疑似被黑，且自动发送垃圾信息。新浪微博方面提醒用户，不要点击此类带有链接的私信或评论，该漏洞暂不会泄露用户新浪微博密码，没有必要修改密码。

据了解，用户中毒后会在短时间内自动发布“建党大业中穿帮的地方”等大量带链接内容，同时会向粉丝发送带病毒链接的私信，中毒用户反映，粉丝一旦点击这些链接，就会感染微博病毒，用已登录的微博账号自动发布病毒微博和私信。

随后中毒用户“安卓论坛”发布微博称，该病毒始作俑者是账号为“hellosamy”的用户，该用户在大量传播病毒的同时强制中毒账号关注自己，在短时间内粉丝数量即超过 3 万。

耀疆点评

技术人员表示，这是由于在生成短链接的时候未能严格检查 script 标签引起的。病毒作者在真正的链接中嵌入了 script，而由于该链接使用的是新浪本地的 url，所以 script 是在本域执行的，可以直接模拟用户的各种请求。

据悉，本次事件采用的是 XSS 攻击，XSS 又叫 CSS (Cross Site Script) ，即跨站脚本攻击。它指的是恶意攻击者往 Web 页面里插入恶意 html 代码，当用户浏览该页之时，嵌入其中 Web 里面的 html 代码会被执行，从而达到恶意攻击用户的特殊目的。在拥有大量用户的基于 WEB 的应用系统中，如果存在 XSS 漏洞并被利用，将引发大量用户执行恶意代码，演变成大范围事件，需要重点防范。

影响范围：★★★★☆
影响程度：★★★★☆
持续时间：★★★☆☆

关键字：

认证机构 颁发虚假认证 安全漏洞

荷兰数字证书机构遭到攻击

信息来源
新浪新闻，
http://tech.sina.com.cn/i/2011-08-31/12096005012.shtml

事件回顾

2011 年 9 月一个化名“IchSun”的黑客实施了对荷兰数字证书机构 DigiNotar 的攻击，导致共有 531 份 SSL(安全套接层)虚假数字证书被颁发出去，其中就包括一份被用于攻击谷歌网站的数字证书。这名黑客还在 2011 年春天策划了对安全数字证书机构 Comodo 的攻击，此人还透露他入侵过其他 4 家知名度很高的数字证书机构，其中就包括 GlobalSign。

DigiNotar 存在多项安全漏洞，包括在最重要的服务器上有恶意软件，装在公共网络服务器的软件过时，缺乏对受影响服务器的杀毒保护等。

英国电信集团的首席安全技术官 Bruce Schneier 指出：“这起攻击表明了 SSL 存在的许多安全问题当中的一个：单一信任点实在太多了。”换句话说，只要破坏了这些信任点中的任何一个，安全也就荡然无存。

耀疆点评

荷兰政府事后委托第三方机构，对这起事件进行了调查。据调查的初步结果显示，DigiNotar 的信息安全工作做得很差劲，包括：没有集中式日志，没有集中管理关键部件，使用过时、没有打补丁的软件，以及管理员密码通过暴力攻击就很容易被破解等。此外，所有的数字证书服务器都同属于一个 Windows 域，那样只要闯入一个管理员帐户，就能控制一切。

影响范围：★★★★☆
影响程度：★★★☆☆
持续时间：★★★☆☆

关键字：

病毒侵袭 Android 系统 安全漏洞

大量病毒侵袭 Android 系统智能手机

信息来源
中国日报，
http://www.chinadaily.com.cn/micro-reading/fortune/2011-11-18/content_4409443.html

事件回顾

2011 年 11 月 16 日，美国 Juniper 网络公司指出，愈来愈多的装载 Android 系统的智能手机和其他智能工具受到了大量病毒程序的侵扰。从 7 月份起，病毒的数量相对以往已经增加了 4 倍。其中半数的恶性病毒是一种间谍程序，目的在于窃取手机用户的私人信息。其他类型的病毒则通过一种特定程序在用户不知情的情况下向未知号码发送短信，而且这些短信的收费一般都极其昂贵。

耀疆点评

这次 Android 系统病毒扩散的主要原因在于其开源式的商业模式，大量第三方应用商店的存在导致 Android 应用软件安全性难以保障。相比苹果操作系统，Android 相对较为开放，可被第三方修改，缺少一个可以控制系统适用性范围的程序，因此木马和病毒很容易进入该系统，对客户的隐私和财产造成损害。

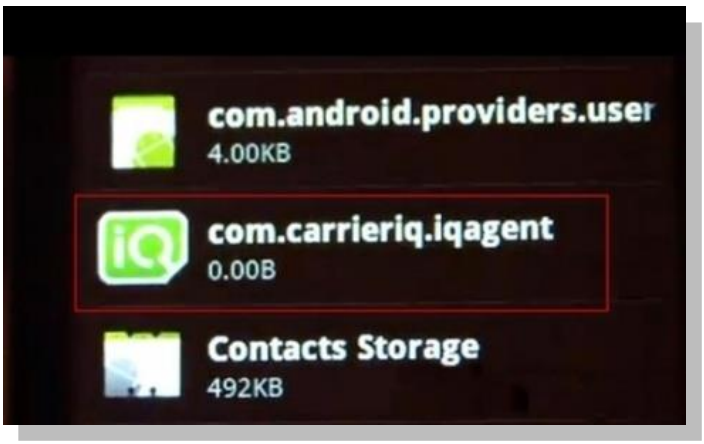
国内之前也曾出现过利用“吸费短信”来骗取用户高额的国际短信费的案例，但相比之前的“吸费短信”，针对 Android 系统的病毒更令人堪忧。Android 系统是目前市场上发展最为迅速、用户使用数量最多的手机及移动终端操作系统之一，此次事件直接引发了广大公众对于智能手机/智能终端等电子设备安全性的担忧。

影响范围：★★★★☆
影响程度：★★★☆☆
持续时间：★★☆☆☆

关键字：

运营商 捆绑软件 窥探隐私

美移动运营商安装窥探用户隐私软件



事件回顾

据国外媒体报道，一款名为“CarrierIQ”的手机应用软件今日登上了各大新闻媒体科技板块的头条。尽管只是一款手机程序，但它却先后引发了黑莓生产商 RIM、HTC、诺基亚，甚至最后才站出来的苹果纷纷公开发表声明——与之撇清关系。这些往日争得面红耳赤的智能手机生产商们，今天却首度破天荒地站到了一起，共同抗敌。

CarrierIQ 为何物，竟有如此巨大影响力？实际上，位于美国加州的 CarrierIQ 开发商背景并不强大，不过由于该软件能大量收集用户数据，甚至能监视用户行为，从而大受移动网运营商欢迎。安全研究人员发布报告称，CarrierIQ 软件可以收集用户数据，包括用户所处的位置、键盘录入情况，以及手机运行的程序。用户通常并不知晓自己的手机安装了这款软件，而且无法关闭它。

而 HTC 更是将矛头直指美国移动网运营商：“CarrierIQ 是美国好几家移动网运营商指名安装的软件。所以，任何媒体或用户如有任何关于 CarrierIQ 如何工作、收集了哪些数据的问题，我们建议请直接质问这些运营商们。”

耀疆点评

新商业模式对隐私保护的侵犯：随着越来越多装载 IOS、Android 等操作系统的智能手机或便携电子设备进入广大公众的生活并快速普及，这些设备在给普通人带来生活乐趣和便利的同时也带来了信息泄漏的隐患，普通民众对于智能手机操作系统并不熟悉，各类预装或者自行安装的软件完全有可能在无形中泄漏用户的个人信息，用户在使用相关软件前有必要确认其是否可能造成自身信息的泄漏。

信息来源
网易，
http://tech.163.com/11/1202/07/7K8L0JSH000915BE.html

影响范围：★★★★☆
影响程度：★★★★★
持续时间：★★★★☆

关键字：
CSDN 用户信息泄露
600 余万 密码明文 天涯 4000 万

CSDN 等多个网站用户信息泄漏

事件回顾

2011 年 12 月 21 日下午，全球最大中文 IT 技术社区 CSDN 网站的用户数据库被泄露，导致包括 600 余万个明文的注册邮箱账号和密码被公开上传下载，在包括新浪微博在内的平台上广泛传播后，前晚，CSDN 在其官方网站和微博上对此予以确认，并发布致歉信。

“我们非常抱歉，近日发生了 CSDN 用户数据库泄露事件，您的用户密码可能被公开。我们恳切地请您修改 CSDN 相关密码，如果您在其他网站也使用同一密码。请一定同时修改相关网站的密码。”在致歉信中，CSDN 申明：对于 CSDN 用户账号密码数据库被泄露一事，经过初步分析，该库系 2009 年 CSDN 作为备份所用，由于未查明原因被泄露，特向所有因此而受到影响的用户致以深深歉意。

耀疆点评

业内人士爆料，有更多网站的用户资料遭到黑客疯狂盗取并被转手卖钱，一些重要的数据包甚至可以卖到上百万元。

网络专家建议所有采用弱密码的用户以及所有网站使用同一用户名和密码的用户尽快修改。首先，使用至少 2 个邮箱来绑定或申请网络服务，并确保邮箱密码不重复使用。其次，重要服务用重要邮箱来申请，一般服务用次要邮箱来申请。再次，尽量不重复使用重要服务的密码，并定期更换。

信息来源
网易，
http://tech.163.com/11/1223/02/7LU5RGHI000915BF.html

重大经济损失类

造成重大经济损失的信息安全事件

本文收录了9个具有典型意义的经济损失类信息安全事件，包括瑞银交易员违规操作致20亿美元损失、中国银行网银用户遭遇升级骗局、韩国农协银行系统遭攻击、亚马逊云服务发生中断、广发银行系统漏洞导致盗刷信用卡、花旗银行网站遭黑客攻击、支付宝用户被捐款、郑州商品交易所系统故障致交易暂停、港交所网站遭黑客攻击个别股票停牌等。

重大经济损失类信息安全事件是指由于信息安全事件的发生对国家、企业、组织造成重大经济损失，或消除安全事件负面影响使国家、企业、组织付出重大经济代价的信息安全事件。

在 2011 年的一年中，除了危及国家安全、产生重大社会影响的各类信息安全事件，还有很多由于信息安全问题导致的重大经济损失事件，其中最为典型的就是与在线支付安全及商业秘密保护相关的信息安全事件，而这些事件的发生多数是受到了经济利益的驱使。

在线支付在广大公众日常生活中的使用频率已经越来越高，从早先的网络购物到如今的订票、购物、缴费等各类在线支付活动。在线支付对于公众日常生活的影响已经越来越大，网上购物几乎已经成了日常生活中不可或缺的一部分。在线支付在给生活带来巨大便利的同时，同样也来带了相应的风险。2011 年国内外发生了数起与在线支付及商业秘密保护相关的信息安全事件，如国内最大第三方支付公司“支付宝”用户莫名其妙发生“被捐款”事件、日本军工生产企业三菱重工旗下打造潜舰、生产导弹、以及制造核电站零组件等工厂的电脑网络遭到黑客攻击事件等。

移动互联网、云计算等技术的迅速发展改变着传统的商业运作模式，高效的信息获取和处理是现代企业在竞争激烈的商场上获胜的重要法宝之一。越来越多的商业机密通过信息网络来进行处理、传输和存储，由于信息安全事件导致的商业机密泄露问题十分突出。2011 年发生了多起银行系统或交易系统被攻击而造成商业机密泄露的事件，如花旗银行大量用户信息泄露、港交所网站遭攻击导致部分股票停牌等。

与经济利益相关的信息安全保障要从管理和技术的多个角度来进行综合防护。在线支付的安全，不仅仅是支付机构的安全防护，也需要政府和媒体的正确引导、行业监管和指导以及用户自身安全素养的提升。同样，商业秘密保护的建设也是一个系统工程，它需要对涉及商业秘密的各个环节进行统一的综合考虑、规划和构架，并要时时兼顾组织内不断发生的变化，任何环节上的安全缺陷都会对构成对系统的威胁。

影响范围：★★★☆☆
影响程度：★★★★★
持续时间：★★☆☆☆

关键字：

瑞银集团 违规交易 20 亿损失

瑞银交易员违规操作致 20 亿美元损失

事件回顾

2011 年 9 月 15 日，瑞士银行爆出惊人消息，该行一名自营业务操作员因涉嫌违规交易，导致该行金融衍生品自营业务亏损 20 亿美元。

瑞士银行集团因交易员违规操作致损 23 亿美元事发仅 9 天后，瑞银董事会即宣布首席执行官奥斯瓦尔德·格吕贝尔已引咎辞职，给危机频发的瑞银带来新的打击。有分析认为，瑞银违规交易事件不仅使自身面临一场史无前例的信任危机，更使欧洲银行业的融资困境雪上加霜。

耀疆点评

侥幸心理也是此类“奇迹”频发的重要因素。金融界成功的标尺并非帮助银行、客户避免了多少损失和风险，而是利润和利润率，“以小搏大”可以快速成功的衍生交易，自然成为急欲上进的中低层操作员最青睐的品种。在这些“奇迹”中，不少操作者本人并未从交易中直接获利，其唯一动机是通过捷径博取业绩，在银行出人头地，而他们的专业知识又足以让其熟知规则和漏洞，可以较长时间地躲避监督检查。不仅如此，在激烈的竞争和低迷的世道压力下，银行本身明知衍生交易风险大、监管难，却仍然乐此不疲，甘愿冒险。

信息来源
新浪财经，
http://finance.sina.com.cn/stock/usstock/c/20110915/200610487254.shtml

影响范围：★★★★☆
影响程度：★★★★★
持续时间：★★☆☆☆

关键字：

中国银行 网银骗局 5万用户

中国银行网银用户遭遇升级骗局

事件回顾

2011 年 1 月，许多人都收到了一条来自 13225870398 发来的短信，称中行网银 E 令已过期，要求立即登录 www.bocc.nna.cc 进行升级。金山网络安全中心 20 日发布橙色安全预警称，这是不法分子冒充中国银行以中行网银 E 令(网上银行动态口令牌)升级为由实施的网络诈骗，此类诈骗手法将传统的短信诈骗与钓鱼网站相结合，欺骗性更强。

据一位向公安机关报案的黄姓网民称，在收到短信后，登录短信中指示的网址，输入银行卡号和密码，即被提示升级成功，但随后发现卡上的 16000 元现金已被转走。据《钱江晚报》报道，绍兴市民章某在接到短信后，登录假冒的中行网站，约 48 秒后 100 万元即被偷走。无独有偶，当地的魏先生、陆先生也分别被相同骗局骗走了 1700 元和 11 万元。

安全专家表示，这是一起典型的网络诈骗案，犯罪分子利用互联网和现代通讯手段，冒充中国银行发送短信，以中国银行系统升级或事主办理的中行网银动态口令牌需要立即升级为由，让其登录假冒的中国银行网站(www.bocpu.tk、www.bocc.nna.cc)，并要求事主在假冒网站上输入银行卡号和密码，一旦事主按照提示进行操作，事主的网银用户名、密码及动态口令即被盗取，卡内现金也被悉数转走，同时该假冒网站立即消失。

耀疆点评

中国金融认证中心相关负责人告诉记者，目前用户端网银安全工具主要包括：数字证书、动态口令、手机验证三种。得到广泛使用并且安全保障程度较高的是数字证书，通常被存储在USBKey(俗称的“U盾”)之中。用户在登录银行网站进行交易时，在电脑上插入Ukey，就相当于向银行亮出“网络身份证”。

中国银行选择的是用动态口令保护用户网银安全。动态口令就是只能使用一次的密码，这种动态密码的原理在于：它通过特定的计算方式在用户处产生一个随机变化的密码，同时银行处也能产生一个相同的密码，用户使用这个密码登录网银时，两个密码相比较，若匹配则表示已通过验证，用户可进行下一步的操作。

中行“E令”，实际上就是“电子动态口令生成器”，是由中国银行推出的一种硬件动态口令牌。它由内置电源、密码生成芯片和显示屏等组成，根据专门的计算法则，每隔60秒会自动更新一个动态口令，要求用户在60秒内输入，以保障网银操作安全。然而此次网银诈骗事件，绝大部分案例都以“中行E令”为幌子，众多用户质疑号称动态安保的“中行E令”此时已形同虚设。

信息来源
新浪，
http://finance.sina.com.cn/money/bank/guangjiao/20110121/08229289777.shtml

影响范围：★★★★☆
影响程度：★★★★★
持续时间：★★★☆☆

关键字：

韩国 农协银行 黑客攻击 系统瘫痪 数据丢

韩国农协银行系统遭攻击

事件回顾

2011 年 4 月，韩国农协银行疑遭电脑黑客袭击，其电脑网络瘫痪了三天，数以万计的客户受影响。

韩国农协银行有约 5000 家分行，拥有韩国境内最大的银行网络。4 月 12 日，该银行电脑网络开始出现故障，客户无法提款、转账、使用信用卡和取得贷款。三天后，农协银行才恢复部分服务。

在事件发生期间，农协银行接到大约 31 万名客户的投诉，另外还有将近 1000 人要求银行赔偿。农协已承诺将对客户所蒙受的损失作出全额赔偿，同时也强调客户的个人资料并没有因为这起事件而泄露出去。

耀疆点评

农协银行领导层怀疑，其网络瘫痪是黑客造成的。当局怀疑黑客输入指令，将银行的电脑服务器破坏，并消除部分的交易纪录。据了解，大约 540 万名信用卡客户的交易记录已被暂时删除。

韩国检察官正在调查这起事件是否是黑客所为。韩国金融监督院及中央银行官员则前往农协总部调查该银行是否遵守电脑安全规则。

农协银行职员金友庆表示，这事件可能是一名“有经验”的专家所为，使得银行的整个网络陷入瘫痪。他指出，这名黑客利用分包商的笔记本电脑输入指令，破坏了整个服务器系统。

信息来源
中国计算机安全，
http://www.infosec.org.cn/news/news_view.php?newsid=14473

影响范围：★★★☆☆
影响程度：★★★☆☆
持续时间：★☆☆☆☆

关键字：

亚马逊 云服务 服务中断

亚马逊云服务发生中断

事件回顾

2011年4月22日著名的云计算服务提供商亚马逊表示，其网络服务（Web services）4月21日上午出现的技术故障依然未彻底解决，服务中断已超过24小时，不过该公司预计可在当地时间周五下午解决。亚马逊称，网络服务的故障修复工作已经取得进展。有些网站正在等待亚马逊服务的全面恢复，有些网站由于无法使用该服务而采取了应变计划。亚马逊一直宣称云计算服务是企业外包数据中心的廉价而安全的途径，但本次事故再一次提醒业界使用这种服务存在的风险。

基于位置的移动服务网站Foursquare、问答服务网站Formspring.me和新闻聚合器网站Reddit.com，都指责这次事故导致他们的网站运营中断。此外，亚马逊的云客户还有Netflix、礼来公司（LLY）和互联网游戏公司Zynga等，也受到不同程度的影响。

这次故障也使一些公司的网站崩溃，这些公司是帮助企业开发运行在亚马逊云计算中的工具。例如Salesforce.com的Heroku网站停止运营已超过八个小时，Heroku是帮助百思买和Comcast等公司开发在亚马逊服务中使用移动和社交网络应用的网站。

耀疆点评

目前企业对云计算抱有浓厚的兴趣，由于云服务可以使企业通过互联网和内部网络访问电脑服务器和储存数据，从而降低了各公司搜集数据的成本并且能更灵活地处理数据内容，但是这也带来了需要依靠第三方解决潜在问题的风险。

此次故障的争论中心在于，亚马逊为什么没有能力设置多个信息库并联处理，从而避免出现一个数据库故障就导致整个系统全军覆没的情况发生，确保其客户网站正常运转。

云服务近期正受到追捧，很大程度上是因为云服务的安全性和可靠性，然而此次的亚马逊事件使得广大公众以及对于云服务有着较高期望的业内人士产生了怀疑，云服务是否真的如之前所描述的那么美好？在云服务日渐普及的今天，如何才能确保云服务的可靠与安全，这都是广大服务提供商面临的一大考验。

信息来源
网易，
http://tech.163.com/11/0422/06/727M5FEG000915BF.html

影响范围：★★★☆☆
影响程度：★★★☆☆
持续时间：★★☆☆☆

关键字：
广发银行 网银漏洞 信用卡盗刷

广发银行系统漏洞导致盗刷信用卡

事件回顾

2011 年 5 月 20 日，广发银行信用卡的新网银系统上线，其中一项重要修改是，取消原有固定的支付密码，而采用手机动态密码的方式，也就是说，每次支付前，手机将收到一条动态密码，以此作为支付凭据。但由于新老系统升级过程中，系统衔接出现问题，导致如果用户在老系统中没有设置“私密问题”的话，黑客只需知道网银登录名和密码，便可在网银上修改卡号所绑定的手机号码，从而使修改后的密码直接发送至新手机上，采用新手机上收到的动态支付密码完成支付。

据统计，有 12 名用户因此遭到信用卡盗刷，受害人的信用卡都是在上海环迅电子商务有限公司这个第三方支付平台上被盗刷的，被盗资金都被转入滕驰策划公司。12 人中，除叶先生的手机动态验证码被修改为 138 开头的手机号外，其余人的号码全部被修改为 159 开头的特定号码，且都为北京号码。

耀疆点评

作案者手段几乎一致：在受害者网银中修改手机号码，利用新号码接受动态密码，从而完成盗刷支付。近 10 名被盗刷者提出的相同问题是：网上支付环节中最重要的一环——手机号，为什么能如此轻易修改？第三方支付平台能否提供更多的风险控制功能？

目前国内信用卡交易所采取的安全技术措施包括静态口令、动态口令、USB 令牌、数字证书、手机验证码等，从此次事件来看，以往一直被认为较为可靠的手机验证码措施并非无懈可击，相较而言，采用 USB 令牌或数字证书验证的手段从目前来看安全性似乎更高一些。

如何有效确保众多持卡人及网银用户的用卡安全，将是各家银行今后面临的重大挑战之一。

信息来源
新浪科技，
http://tech.sina.com.cn/t/2011-08-29/08245992725.shtml

影响范围：★★★★☆
影响程度：★★★☆☆
持续时间：★☆☆☆☆

关键字：

花旗银行 黑客攻击 20 万用户 信息池

花旗银行网站遭黑客攻击

事件回顾

2011 年 6 月花旗银行报告说，该银行网站遭遇黑客袭击，大约 20 万名用户的信用卡和个人信息被盗，其中包括用户的姓名、帐号、家庭住址和电子邮件地址等。报告中说，被盗的帐户主要是北美地区的信用卡用户。

花旗银行报告中说，黑客非法侵入了该行的计算机系统，浏览或拷贝了大约 20 万名信用卡用户的个人信息。花旗银行在北美地区有大约 2100 万名信用卡用户，被黑客盗取信息的用户数量约占用户总数的 1%。

花旗银行并没有透露网站如何受到攻击的详细信息，但称是在每日例行检查中发现了这一问题。社会保险号、出生日期、银行卡有效期等客户信息并没有泄露。花旗北美零售银行有关负责人表示，花旗银行已经升级程序以防止此类事件的再度发生。同时，大部分在这起资料遭窃事件中受到影响的信用卡将进行更换，以维护用户的安全。花旗银行中国有限公司昨天接受媒体采访时表示，花旗中国的客户资料没有泄露，并未受到任何影响。

耀疆点评

业内人士称，虽然黑客并没有获得银行卡用户完整的信息，但已获得的联系方式已经足够使恶意攻击者有办法获取更多的信息。例如邮箱地址可以用来发送“钓鱼”信息，还可以通过电话冒充某个权威机构的工作人员，使受害者“自愿”泄露个人信息。此外，银行还发现一些用户的信息被非法修改，个别用户名下出现了多个信用卡账号。这可能导致信用卡资金在用户不知情的情况下被转移。

信息来源
中国经济网，
http://intl.ce.cn/specials/zxxx/201106/10/t20110610_22473417.shtml

影响范围：★★★☆☆
影响程度：★★★☆☆
持续时间：★☆☆☆☆

关键字：
支付宝 资金安全 被捐款

支付宝用户被捐款

事件回顾

2011 年 8 月以来，国内最大第三方支付公司“支付宝”用户发生“被捐款”事件。

网名为“蝌”的网友在天涯发帖称，自己突然发现支付宝账户少了 6000 多元钱，经查从 9 月 26 日起，其支付宝账户中的钱被莫名其妙地一笔一笔捐到了“绿化基金会”。拥有同样经历的网友不在少数，每次捐款金额大多在几毛钱到几十块钱之间不等。几毛钱、几块钱的小额“捐赠”，引发公众普遍关注，形成支付宝“被捐款”事件。

第三方支付公司如支付宝等支付账户使用邮箱注册，但其属性却类似于银行账户，可以进行涉及资金的操作。而且，部分用户对待这些支付账户，安全意识并没有提升到银行账户高度，而是与一般 SNS、微博邮箱等同看待。

这样会留下较大隐患。据研究表明，黑客团伙会攻击并盗取一些安全防范较弱的小型网站用户资料，如 SNS 网站，然后使用账号与密码逐一尝试登录网络支付平台，如用户采用了相同的账号设置，账户资金容易损失。出于省事的考虑，不少用户除了使用同样的账户名外，还将微博、邮箱和

网络支付账号都使用相同的密码，为账户资料甚至是账户资金被窃埋下极大的安全隐患。

对此，支付宝已向用户发出警示，由于涉及资金安全，请用户务必为支付宝账户设置单独的高强度密码，并使用数字证书、支付盾或宝令等安全产品。网上购物过程中，不要轻易点击不明链接或安装不明文件。

耀疆点评

中国电子商务协会政策法律委员会副主任阿拉木斯认为，“在网民反映的‘被捐款’事件中，应该说，支付宝已经尽到了责任义务。”阿拉木斯说，根据国内有关第三方支付的法规，数字证书等安全产品并没有强制使用，如果密码简单、点击木马或钓鱼网站，账号被盗用的概率很高，“账户安全关系到用户自身利益，如果大家一方面认为网上支付不安全，但又不用现有的安全产品，可能埋下隐患，毕竟越方便有可能就越不安全。”

但一些网民认为，即便已经提供了安全服务，相对于网购和支付平台，普通用户不论在技术还是信息获取上，都处于弱势，平台可以提高技术安全防范能力，并增强对安全使用和付款情况的实时提醒。

就整个第三方支付平台而言，不论是技术支撑还是服务提醒，都还有提升空间。另外，国内相关管理规范仍然过于笼统，也可能产生问题。快速发展的第三方支付市场需要多方努力完善，避免触发安全隐患。

信息来源
网易财经，
http://money.163.com/11/1101/08/7HOU07MG00252V0H.html

影响范围：★★★☆☆
影响程度：★★★★☆
持续时间：★☆☆☆☆

关键字：

港交所 黑客攻击 股票停牌

港交所网站遭黑客攻击个别股票停牌

事件回顾

2011 年 8 月 10 日中午，香港交易所公布上市公司信息的平台“披露易”网站疑因黑客入侵服务出现不稳定情况，投资者难以在网站上获得上市公司发布的股价敏感信息，结果引发 7 间上市企业午后集体停牌。

港交所指出，被停牌的企业一共有 7 家，包括港交所、汇丰控股、国泰航空、大新金融、大新银行、华润微电子和中国电力，港交所的其他系统未受事件影响，旗下证券及衍生产品市场交易继续如常进行。

时任香港政务司司长的唐英年对事件表示关注，并致电港交所主席夏佳理了解情况。唐英年表示，期望港交所从速完成维修，尽快恢复正常运作，同时找出故障原因，避免事件再发生。

耀疆点评

港交所决定当日中午休市期间将要发布公告的 7 家公司停牌，包括中国电力(China Power International)和国泰航空(Cathay Pacific)。香港股市流动性最高的股票汇丰控股也被停牌。

有经纪公司对媒体称，由于停牌过于突然，部分投资者可能担忧无法平仓，被迫承担隔夜风险。此外，400多只权证对应的正股意外停牌，也可能令权证发行商无法及时进行对冲操作，承受相当风险。

事实上，港交所早先已经承认系统等基础设施已显陈旧。在其《战略规划 2010-12》中提及的改革措施就包括提升信息技术基础设施，而此次系统故障，或许为港交所改革的进一步推动铺平道路。

股票交易具有实时性强、涉及金额大、风险高的特点，通过攻击股票信息发布平台导致投资者无法获取上市公司股价敏感信息是一种针对股票交易的特定攻击手法。

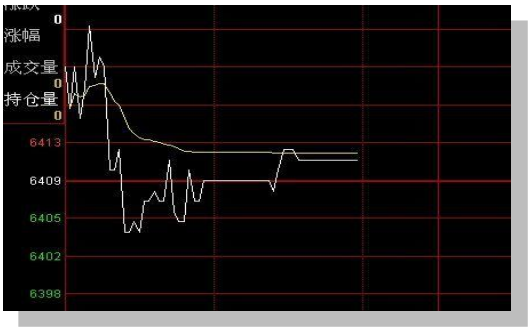
信息来源
新浪网，
http://news.sina.com.cn/c/2011-08-11/140522974276.shtml

影响范围：★★★★☆
影响程度：★★★★★
持续时间：★☆☆☆☆

关键字：

郑州期交所 系统故障 交易暂停 期货价格波

郑州商品交易所系统故障致交易暂停



信息来源
网 易 财 经 ，
http://money.163.com/11/1207/10/7KLQT7LO00252895.html

事件回顾

2011 年 12 月 7 日周三上午，郑州商品交易所期(郑商所)交易行情两度中断，造成客户无法交易，随后郑商所发布公告，称因技术型原因导致交易暂停。午后郑商所再度发表公告称技术性故障已经排除，从 13:30 起恢复正常交易。

据悉本次郑商所系统瘫痪为近年来罕见事故，因为根据相关业务规则，当主系统出现故障时，应尽快切换到冗余系统，确保交易正常进行。

这次事件致使各家期货公司当天纷纷向客户发出建议：“立刻平仓郑商所的交易品种，防止事故下午再次发生。”当天下午开盘后，白糖主力 1205 合约在短短的十分钟内，便由每吨 6423 元跌至 6386 元/吨；郑棉主力 1205 合约六分钟内从每吨 20625 元跌至 20580 元/吨。

耀疆点评

在所有金融交易中，期货交易对于实时性的要求最高，哪怕只是 1 秒钟的差异，也可能导致动辄上千万的损失，因此相比较股票交易系统、银行资金系统而言，期货系统对于系统实时性的要求更高。

此次郑州期交所的事件直接暴露了期货交易所在业务连续性管理方面的不足，根据常理推断，在交易系统出现故障后，并未能在第一时间切换到备用系统。