2016年七大数据泄露事件

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	The 7 Most Sensational Breaches Of 2016		
原文作者	Ericka Chickowski	原文发布日期	2016年12月6日
作者简介	Ericka Chickowski专攻信息技术和业务创新方向，定期为Dark Reading编写安全领域的文章。http://www.darkreading.com/author-bio.asp?author_id=962		
原文发布单位	Dark Reading		
原文出处	http://www.darkreading.com/endpoint/the-7-most-sensational-breaches-of-2016/d/d-id/1327636		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

2016 年七大数据泄露事件

Ericka Chickowski

2016 年 12 月 6 日

本文将介绍 2016 年使公司和政府机构焦头烂额的、最严重的黑客攻击，数据泄露和盗窃事件。

还记得当初，我们认为数亿人的信用卡号被盗已经是最糟糕的企业攻击事件了。如今看来这种想法实在太天真了。在 2016 年，大规模的数据泄露事件大幅减少。单从数字上看，今年的数据泄露事件并不惊人，但是它们的影响却更加严重。2016 年，最具影响力的黑客攻击和数据泄露事件直接导致了数千万美元的诈骗汇款，可能影响了美国大选，还导致了企业高管引咎辞职。

1. IRS

近年来，IRS（美国国家税务局）退税诈骗事件不断增加，所以当今年全面进入纳税季时 IRS 宣布它遭到了攻击也就不足为奇了。这次攻击使 IRS 的反欺诈措施备受怀疑。IRS 报告说，犯罪分子破坏了它的电子提交 PIN 码重置系统，窃取了超过 10.1 万个 PIN 码，企图控制纳税人的账户并提交诈骗性退税申请。

2. 雅虎

虽然 2016 年的大规模数据泄露事件减少了，但是雅虎不幸地成了一个例外。今年 9 月，雅虎宣布在一次大规模数据泄露事件中，超过 5 亿用户的账户凭证被盗。此次数据泄露的原

因仍然不明，但是我们已经知道，该事件是发生在 2014 年的，只是发现得晚。因为该事件，雅虎已经面临了 23 项集体诉讼。

3. DNC 黑客攻击

DNC（民主党全国委员会）电子邮件系统遭入侵以及随后的维基解密数据公开或许是最近 10 年中最具影响力的数据泄露事件之一，该事件具有广泛的政治影响。幕后黑手究竟是俄罗斯黑客，Guccifer 还是其他任何人，目前仍无定论，但是 DNC 的安全措施太差，幕后黑手可能是任何人。不管是谁泄漏了电子邮件，这些邮件的内容包含大量对希拉里·克林顿不利的信息，许多专家认为该事件导致了希拉里在总统大选中的垮台。

4. 伊利诺伊州和亚利桑那州选举委员会

谈到网络犯罪对选举的影响，专家们仍在试图了解针对伊利诺伊州和亚利桑那州的选举委员会的一系列攻击的影响。伊利诺伊州证实，黑客入侵了一个包含多达 20 万选民的信息的数据库，包括姓名、地址、性别、生日、社保号和驾照号。亚利桑那州也出现了类似的数据泄露事件，不过该州的官员没有透露有多少选民受到了影响。这些攻击紧跟饱受争议的总统大选，将会影响大选结果。特别是，一些专家怀疑这些攻击出自俄罗斯黑客的手笔。

5. SWIFT 网络

今年初，孟加拉国中央银行被一个胆大包天的网络攻击组织打劫，攻击者利用欺诈性汇款请求成功地转移了 8100 万美元。但在接下来的几个月中，《路透社》报道称，该攻击是更大规模的攻击活动的一部分，这些攻击活动旨在破坏全球银行使用的 SWIFT（环球银行金融电信协会）通信系统，从而发送汇款指令。调查人员一直在调查十几家银行的攻击事件，SWIFT 也在努力完善成员银行的安全措施，防止孟加拉国中央银行的悲剧再次上演。

6. 旧金山市交通局

2016 年充斥着勒索软件感染事件。攻击者越来越有创意，获得的利润也越来越高，这一点可以通过旧金山市交通局攻击事件得到印证。攻击者不仅窃取了该机构的员工和客户的个人信息，而且还将其信息亭和计算机锁定了两天，迫使该机构在此期间提供免费乘车或中断服务。

7. FACC

FACC（菲舍尔未来先进复合材料股份公司）攻击案例能够在未来几年为安全厂商提供大量的营销噱头。FACC 是波音公司的一家供应商，它遭受的一次鱼叉式网络钓鱼攻击导致 5500 万美元的资金被转走。此次攻击事件导致该公司的股票大跌，并彻底摧毁了该公司 2016 年的盈利能力。从导致的后果上看，这是史上最糟糕的安全事件：数千万美元被盗，首席执行官和首席财务官引咎辞职。而该事件的根本原因是管理人员被简单的社会工程手段（电子邮件）所骗。