简译版

本年度重大云存储泄露事件

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	Major Cloud Storage Security Slip-ups this Year		
原文作者	Kelly Sheridan	**原文发布日期**	2017 年 10 月 13 日
作者简介	Kelly Sheridan 为 Darking Reading 副主编。https://www.darkreading.com/author-bio.asp?author_id=837		
原文发布单位	Darking Reading		
原文出处	https://www.darkreading.com/cloud/10-major-cloud-storage-security-slip-ups-(so-far)-this-year/d/d-id/1330122		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
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。		

继 Verizon，Deloitte 与 Dow Jones 之后，Accenture 的敏感云数据也遭到了泄露。

由亚马逊网络服务 S3 存储桶错误配置引发的云数据泄露是 2017 年令人担忧的问题之一。今年许多公司出现数据泄露，最近的则是 Accenture 泄漏事件。

RedLock 创始人兼 Accenture 首席执行官 Varun Badhwar 指出："虽然此次事件非常不幸，但并不令人意外。"

RedLock CSI（云安全情报）研究表明，53%的使用云存储服务（例如 AWS S3）的公司，曾无意间向公共网络泄露了一次或多次这种服务，这一比例从 5 月份的 40%增加到 53%。研究人员还发现 38%的公司的公共云管理账户曾遭到入侵。

该趋势表明，各种规模的企业以及企业将敏感信息委托给的第三方普遍存在安全问题。很多公司的云存储账户配置方法不当或者未对第三方公司的安全规则进行确认。因此导致客户数据泄露。

今年 6 月份，第三方配置错误导致美国共和党全国委员会（RNC）选民数据泄露。Viewpost 首席安全官 Chris Pierson 指出："虽然可以离岸外包或外包任务与职能，但无法外包风险。"

"因此，每一家处理敏感或有价值数据的公司都应该有一个信息保障计划来对其供应商进行风险评估，监测其安全状况以及其它因素，并给公司提供关于第三方和风险方面的指导。"

在下文中，我们概述了今年十大 AWS 泄漏事件（排名不分先后）。

Accenture

UpGuard 网络风险小组最近发现，Accenture（埃森哲）公司留下了至少四个不安全 S3 存储桶并可供公开下载。Accenture 的疏忽泄露了验证凭证、机密 API 数据、数字证书、解密密钥、客户信息和其它可用于攻击 Accenture 及其客户的数据，其中包括 94 家"全球 100 强"和超过 75% 的全球 500 强公司。

在四个被泄露的服务器中，最大的为 137 GB，被配置为公共访问，并可供任何人输入存储桶网址进行下载。所有这些都包含了有关 Accenture 云平台和使用它的客户的高度敏

感数据。一个文件夹包括一个纯文本文档，其中包含 Accenture 账户的主访问密钥（AWS 密钥管理服务），从而使未公开的凭据变得易受攻击。

UpGuard 说，这一错误可能会导致 "巨额" 的经济损失。攻击者可以使用密钥冒充 Accenture 员工，并留在公司的网络中收集数据，或在多个平台上启动密码重用攻击。

Viacom

Viacom（维亚康姆）是全球第六大媒体公司，价值 180 亿美元，内部访问凭证和其他重要数据被公开泄露，可通过 AWS S3 云存储桶下载。这可能让攻击者接管其 IT 基础设施或互联网广告。

这个错误是 UpGuard 网络风险研究总监克里斯维克力发现的，泄露了一个主资源调配服务器运行傀儡，和需要建立和管理维亚康姆服务器横跨其子公司和品牌的凭证。更重要的是，它泄露了维亚康姆的秘密云密钥，这使得攻击者能够接管其基于云的服务器。

泄露这些信息可能会危及维亚康姆的服务器、存储或数据库，以及维亚康姆使用的几个云实例，包括泊坞窗、Splunk、新遗物和詹金斯。UpGuard 表示，维亚康姆不仅在这一级别存在的数据泄露，但重要的是，它留下了如此敏感的内部数据，对公众开放。

Verizon 的客户 UpGuard 报告了此次泄露事件，指出 1400 万人受到影响，但 Verizon 声称只有 600 万人的数据被泄露了。

据报道，由 NICE 系统工程师管理的基于云的文件库被创建用于记录客户呼叫数据。Verizon 使用公司后台服务和呼叫中心操作。UpGuard 指出存在客户电话号码及其相关 PIN 号码尤其令人堪忧。有了这些信息，攻击者就可以冒充客户获取账户访问权限。

此事件表明依赖第三方供应商处理敏感数据的危险性。NICE 系统配置了存储库以允许公众访问;它完全允许公众下载。

Booz Allen Hamilton

UpGuard 维克力发现情报和国防承包商博思艾伦汉密尔顿 6 万个文件可公开访问 S3 存储桶。大约 28GB 的数据缓存包括高级工程师凭证、美国政府系统密码，以及 6 个未加密的用于持有绝密设备清除权限的政府承包商的密码。

这些档案提及了美国国家地理空间情报局（NGA，一个作战支持机构），它与政府机构，如中央情报局，从间谍卫星和无人驾驶飞机收集地理空间数据。泄露的服务器还具有数据中心操作系统的主凭证，以及用于访问五角大楼系统的其他凭证。

"任何人未经授权都不可访问国家安全信息，这至关重要-在此事发后，排名第一的民主党人在国土安全参议院和政府事务委员会美国参议员克莱尔麦卡斯基尔说到，博思艾伦汉密尔顿把密码和其他敏感信息使得全世界都能看到，。

WWE

早在 7 月，Kromtech 安全研究人员发现世界摔跤娱乐（WWE）存在一个大规模的、未设防的数据库。这些数据存储在 AWS S3 服务器上，它没有用户名或密码保护，任何人都可以访问该网址。

研究人员发现了两个可公开访问的 S3 桶，估计约 12% 的信息被设置为公共访问。第一个不安全存储桶包含了几条 2014-2015 客户的敏感信息，包括姓名，家庭地址和电子邮件地址，生日，教育，年龄，种族，和其孩子的年龄和性别。总记录数为 3065805 条。

第二个存储桶包含另一个数据宝库；这一次从 2016 年和特定的欧洲客户。这包括计费详细信息：例如，地址和用户名，总部涉及数十万人。其它泄露的文件包括电子表格，里面有可追踪 WWE 的社交媒体和一个 Twitter 帖子的缓存。

Dow Jones

Dow Jones & Co 数据泄露了数百万客户的姓名、账户信息、物理和电子邮件地址，以及最后四数字的信用卡号码。这次泄露由 UpGuard 维克力发现的，也影响了道琼斯风险和合规的 160 万项，这是一组在金融公司中使用的用于遵守反洗钱法规的规章。

AWS S3 bucket 中泄露的所有用户数据，都是由于错误配置使得任何 AWS 认证用户都可以使用存储库 URL 下载数据。由于亚马逊将 "身份验证用户" 定义为拥有免费 AWS 账户的任何人，因此该数据可供超过 100 万人使用。道琼斯报道 220 万人受到影响，UpGuard "保守估计" 这个数字高达 400 万。

出版商声称，"没有理由相信"所有的数据被盗，并确认泄露的信息不包括完整的信用卡号码或登录信息，可能给客户带来重大风险。

RNC

RNCDeep Root 分析是一家数据分析公司，代表共和党全国委员会（RNC），通过一个不安全的 AWS S3 存储桶泄露了 1 亿 9800 万美国选民的个人资料。这些被泄露的数据包括生日、电话号码、自我报告的种族背景、家庭和邮寄地址以及党派归属等数以百万计的记录。

Deep Root 存储桶被配置为公共而不是私有，因此，其内容可以在网络上查看。根据 UpGuard 的消息，大多数记录都具有下载权限，并且没有密码就可以访问文件，这也发现并报告了此漏洞。

继 Deep Root 事件之后，专家们警告说，这种信息存在落入坏人之手的危险。Microtargeting 是犯罪分子使用的一个强大的工具，可用于执行鱼叉式钓鱼攻击和社会工程攻击。

TigerSwan

TalentPen，一家负责处理新求职者的第三方供应商，因错误配置的 AWS S3 桶缺乏密码保护导致数以千计的美国个人数据被泄露。在泄露的 9402 份文件中，大部分是个人安全公司 TigerSwan 的简历和申请。

这个错误泄露了某些分级安全审查的绝密个人信息。在安全审查的顶部，这些文件包含了敏感信息，包括驾照号码、护照号码和至少部分社会保险号码。泄密揭露了联合国、美国特勤局、国防情报局、国防部和国土安全部所雇用的国防、情报、执法、语言和后勤专家的工作历史。

UpGuard 发现并向 TigerSwan 报告了泄漏的信息："泄露的文件几乎完全属于美国退伍军人，对其过去的用名提供了详细的信息,包括精英或敏感国防和情报的人物。"

Time Warner Cable

Time Warner Cable（时代华纳有线）泄漏事件凸显了外包的危险，约对美国 400 万时代华纳电缆 （TWC）客户造成了影响。Kromtech 安全中心发现了两个 AWS S3 桶被全球通信软件和服务提供商 Broadsoft 泄露在网上。公司拥有 600 多家服务提供商，并支持数百万订阅用户。合作伙伴包括时代华纳有线电视、AT&T、Sprint 和沃达丰。

在这种情况下，这两个桶包含了 TWC Broadsoft 客户端 "数以千计的记录和报告"。这包括内部开发信息，如 SQL 数据库转储、具有访问凭证的代码和访问日志。一个文本文件包含超过 400 万记录，其中包括用户名、Mac 访问、序列号、账户号和交易 id 等信息。其他数据库有 TWC 客户的地址和电话号码。

两个桶都配置为公共访问；Kromtech 表示，那些从未关闭过公共配置可能已经被工程师遗忘了，因此使得任何人都可以在线访问数据。任何有互联网连接的人都可以访问敏感数据，任何 "经过身份验证的用户" 都可以从 URL 下载数据或使用其它应用程序。

ES&S

UpGuard 发现了此次泄漏事件。著名的投票机器和相关软件提供商 ES&S 错误配置的 AWS S3 桶被泄露并可以公开下载。

此次错误泄露了 180 万芝加哥的个人信息，包括姓名地址、电话号码、驾照号码和部分社保号。泄露的数据库似乎是在 2016 大选期间，芝加哥选举委员会委员们创建的。