多达 10 亿雅虎账户被盗

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	Hackers Breach a Billion Yahoo Accounts		
原文作者	Lily Hay Newman	**原文发布日期**	2016 年 12 月 14 日
作者简介	Lily Hay Newman 是《连线杂志》安全领域的作者。https://www.linkedin.com/in/lilyhnewman/		
原文发布单位	《连线杂志》		
原文出处	https://www.wired.com/2016/12/yahoo-hack-billion-users/		
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。		

多达 10 亿雅虎账户被盗

Lily Hay Newman

2016 年 12 月 14 日

今年 9 月 雅虎因 5 亿用户账户被泄露而受到广泛关注。虽然这一数字骇人听闻 ,但是，雅虎似乎已经打破了这一纪录。雅虎在周三宣布，在 2013 年 8 月的一次攻击中，黑客窃取了该公司 10 亿用户的账户。10 亿啊！这是历史上最大规模的用户数据泄露事件，甩出第二名几条街。

攻击简介

目前，我们知道的最重要的事情是：“此次泄露事件很可能不同于雅虎在 2016 年 9 月 22 日披露的事件。”后者发生在 2014 年底，而前者（规模更大）则更早一年。雅虎一直在与执法部门和第三方网络安全公司合作，以验证攻击事件并追溯其起源。但是雅虎指出，到目前为止，它还不知道攻击者的身份。

雅虎表示，泄露的数据包括用户姓名、电子邮件地址、电话号码、生日、哈希加密的密码，以及加密和未加密的安全问题和答案。如果你心存侥幸，雅虎说被盗的数据不包括未加

密的密码、信用卡号码或银行账户信息。具体来说，金融数据存储在一个单独的系统中，雅虎相信该系统未被入侵。

2015 年和 2016 年，雅虎还发生了数据泄露事件。黑客使用伪造的 Cookie（追踪网络用户的小文件）绕过安全保护并在没有密码的情况下访问用户的账户。雅虎认为，该攻击至少与国家赞助的黑客有些关系，2014 年的数据泄露事件（今年 9 月披露）也是这些黑客的杰作。

21 世纪初担任雅虎信息安全官两年的杰里米亚·格罗斯曼（Jeremiah Grossman，现在是 SentinelOne 的安全战略主管）指出："两三年前，这种事情可能发生在任何人身上，每个人都可能发生重大的数据泄露事件。但是，雅虎数据泄露事件的细节表明，该公司的数据管理存在混乱，安全团队没有获得足够的支持。"

谁受到了影响？

该攻击感染的账户可能与今年 9 月公布的攻击感染的账户存在重叠（甚至很大一部分重叠），但是即使在最好的情况下，至少有 10 亿雅虎账户被黑了。在更坏的情况下，则有 15 亿账户被黑了。2013 年秋，雅虎宣布它的月活跃用户有 8 亿，尚不清楚它到底有多少不活跃的用户。无论怎样，如果你在 2013 年或 2014 年注册了雅虎账户，你都有足够的理由立即重置密码和安全问题。不幸的是，你将无法消除数据泄露造成的损害。"鉴于此次数据泄露发生在三年前，我想知道在过去的三年中有多少泄露事件源于从雅虎窃取的数据。"格罗斯曼说。

有多严重？

我认为真得很严重。考虑到总共有大约 30 亿互联网用户，包括 10 亿活跃用户，因此雅虎花了这么长的时间才发现数据泄露。广泛地看，在过去几年中大规模的企业和政府攻击很盛行，这说明许多机构没有投入足够的资源来保护他们的网络和数字基础设施，他们或者认为不需要，或者认为不能将此优先考虑在预算中，或者认为黑客攻击不会发生在他们身上。雅虎似乎犯了其中一个错误，或者上述所有错误。

虽然密码采用哈希加密，但是该方法存在几个漏洞，这意味着用户并不安全。雅虎表示，他们正在通知受此次数据泄露事件影响的用户，并要求所有用户更改密码。该公司还取消了加密的安全问题，从今年 9 月以来一直鼓励用户放弃使用安全问题。

此次数据泄露不光严重影响了雅虎的新老用户，也可能影响威瑞信对雅虎核心互联网业务的收购。《纽约邮报》曾报道说，今年 9 月曝出数据泄露之后，威瑞信要求雅虎对 48 亿美元的交易折扣 10 亿美元。威瑞信尚未回应周三曝出的两倍大的黑客攻击事件。

希望这是雅虎需要处理的最后一次泄露事件，但是雅虎将难以挽回消费者或企业信任，因为这些泄露事件的全部影响还未体现出来。格罗斯曼说："我们怎么能肯定雅虎真的赶跑了黑客？毕竟黑客们有三年的时间隐藏在系统中呢。我认为，如果雅虎将任务透明化，我们是可以确定的，但是透明化却是很难做到的。"