云存储将成为网络钓鱼攻击的新宠儿

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	Cloud Storage: The New Favorite Target Of Phishing Attacks		
原文作者	Jai Vijayan	**原文发布日期**	2017 年 2 月 7 日
作者简介	Jai Vijayan 是一位经验丰富的技术记者和自由职业作家，目前担任 Computerworld 的高级编辑，研究信息安全和数据隐私问题。 http://www.darkreading.com/author-bio.asp?author_id=1912		
原文发布单位	Darkreading		
原文出处	http://www.darkreading.com/attacks-breaches/cloud-storage-the-new-favorite-target-of-phishing-attacks/d/d-id/1328078?		
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。		

云存储将成为网络钓鱼攻击的新宠儿

Jai Vijayan

2017 年 2 月 7 日

PhishLabs 指出，2016 年的数据显示，针对 Google 和 DropBox 等云存储服务提供商的网络钓鱼攻击将会很快超过针对金融机构的钓鱼攻击。

在威胁源采用的所有复杂的战术、技术和程序中，网络钓鱼仍然是 2016 年最受欢迎的攻击手段。

安全厂商 PhishLabs 在本周发布的网络钓鱼趋势报告中指出，2016 年最大的区别在于，网络钓鱼者不再一门心思地攻击金融服务机构，而是越来越倾向于攻击诸如 Google 和 DropBox 这样的云存储服务提供商。

在 2013 年，仅有 10%的网络钓鱼攻击针对云存储服务公司；但是在 2016 年，这一比例达到了约 22.5%，已经非常接近针对金融机构的攻击比例 23%。这意味着，用户今年可能会收到更多的钓鱼邮件，试图诱骗他们提供云存储的凭证。

PhishLabs 高级安全威胁研究员科瑞恩•哈索德（Crane Hassold）说："在过去的四年里，针对云存储服务的网络钓鱼攻击数量激增。从最近的趋势来看，针对云存储服务的钓鱼攻击很可能会超过针对金融机构的钓鱼攻击，成为 2017 年钓鱼者的首要目标。"

至少到目前为止，几乎所有涉及云存储的网络钓鱼攻击都只针对 Google 和 DropBox。

很多针对云存储提供商的网络钓鱼活动使用了诱饵，声称已经与受害者分享了文档或图片，诱骗他们登录网盘账户进行查看。

此类活动使用的大多数钓鱼网页只是简单地复制了 Google，DropBox 和其他合法网站的网页。即使如此，"这类攻击仍然越来越受欢迎，这说明，钓鱼者能够成功地利用这些缺乏可信度的页面感染受害者。" 哈索德说。

PhishLabs 分析了超过 17 万个域中的大约 100 万个钓鱼网站，以及该公司在 2016 年每个月处理的超过 7800 次钓鱼攻击，在此基础上编写了网络钓鱼趋势报告。其分析显示，网络钓鱼活动正在以惊人的速度增加。

举例来说，2016 年钓鱼网站的数量比 2015 年增加了 23%；针对金融服务、云存储/文件托管、网络邮件/在线、支付服务和电子商务网站的钓鱼邮件数量平均增长了 33%。

PhishLabs 确定了网络犯罪组织在 2016 年用于钓鱼活动的 976 个云存储服务，它们分别属于 568 家公司。

2016 年，钓鱼者的目标数据类型也大大扩展了。除了账户凭证和个人数据，钓鱼者还试图使用钓鱼诱饵获取金融、就业和账户安全数据，如安全问题的答案和母亲的婚前姓名。

勒索软件的最佳拍档

在 2016 年，网络钓鱼仍然是最受欢迎的勒索软件传播方法，其目标包括最终用户系统，企业、政府机构、学校和关键基础设施的系统。

2016 年网络钓鱼威胁激增的一个原因是，越来越多的网站已经接受电子邮件地址作为用户名。

哈索德表示，电子邮件地址作为用户名使得钓鱼者更容易收集钓鱼网站上的所有电子邮件账户的凭证，他们无需再攻击电子邮件服务提供商。

“此外，由于越来越多的网络服务使用电子邮件作为主要凭证，钓鱼者可以对这些毫无戒心的目标执行密码重用攻击，从而大大增加利润。”哈索德说。

用于创建钓鱼网站的工具包或模板很容易获得，这些因素也加剧了这一问题。PhishLabs 的统计表明，目前有超过 29000 个钓鱼工具包（包含模板），它们模仿了超过 300 家公司的网站。许多工具包具备复杂的反检测机制，包括基于 IP 地址、HTTP 引用、主机名、白名单和阻止列表的访问控制措施。

哈索德指出：“关键的问题是，我们为网络钓鱼攻击大规模收集凭证创造了理想的条件。”

过去，钓鱼者专注于获取即时收益（例如追踪和出售金融账户的凭证）；而现在，他们试图以最少的精力获取尽可能多的信息。

他们的目标是“在地下市场以更高的价格出售信息，或利用这些信息进一步攻击二级目标，从而增加其收益。”哈索德说。