2013 年 RSA 大会：

PhishMe 发布应对 APT 的新功能

非官方中文译本•安天技术公益翻译组译注

文档信息			
原文名称	PhishMe Unveils New Features to Address APT at RSA 2013		
原文作者	PhishMe Inc.	**发布日期**	2013 年 2 月 21 日
原文发布单位	PhishMe Inc.		
原文出处	http://finance.yahoo.com/news/phishme-unveils-features-address-apt-150000476.html		
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。		

增强技能将提升联邦机构、全球 1000 强公司及国防承包商的能力，以便其更好地应对当今最新的攻击技术。

弗吉尼亚，尚特利，2013 年 2 月 21 日，美通社--安全行为管理服务（旨在提升员工对钓鱼邮件、恶意软件和路过式攻击的应变能力的服务）领先提供商 PhishMe 公司今日宣布，基于其正在申请的专利的新功能正式可用。这些新增功能包括：PhishMe 高度可见目标标识符、基准测试及新型模拟——Double Barrel（双管猎枪），或模仿攻击者借用频繁信息参与钓鱼会话的能力。

MANDIANT®在描述 APT1 攻击周期时提到“他们以频繁的钓鱼攻击开始”。PhishMe®通过以下方式作出回应：提升客户简单模拟并通过有效的沉浸技术使员工更加熟悉这类攻击的能力。

PhishMe 公司首席技术官及联合创始人亚伦•希格比认为，“攻击者花费大量时间寻找潜在的网络目标并向其发送大量看似更具吸引力的邮件”。“因此，我们引进新的功能，客户可借助这些新功能自动创建钓鱼邮件接收群体（基于该组织内网络上高度可见的员工）。此外，我们还发布一种新型的钓鱼模拟方法，以便用户创建、执行并追踪钓鱼的会话活动。最后，我们引进了一种统计分析声音法，帮助客户针对相同场景下得到的结果进行基准测试。”

高度可见目标标识符：提供公开可用信息进一步定制 PhishMe 仿真钓鱼邮件

Trend Micro®在一篇近期的报道中指出，电子邮件地址和个人信息在互联网上高度暴露的员工更有可能收到定向钓鱼邮件。PhishMe 公司高度可见目标标识符提供信息安全小组模拟黑客点击某个按钮收集数据的技术的能力。通过这一功能获取的电子邮箱地址和其他信息可被用于针对独特的接收人量身定制钓鱼邮件。

基准测试：跨产业匿名比较用户对钓鱼攻击的敏感度

这种新的测试功能允许用户运行相同的场景并将所获结果进行匿名比较。PhishMe 是唯一一家拥有如此庞大客户群的公司，以便提供统计分析声音结果的能力。“我以 PhishMe 成长如此之快，可分享钓鱼邮件数据感到自豪。比较单独的场景运行结果仅是一个开始，”希格比补充道。“随着数据集的不断增大，我们将继续解锁有意义的基准测试以便企业比较各自的警觉度。”

双管：复制“双管齐下”的会话钓鱼邮件以访问敏感数据和企业网络

MANDIANT®报告中描述的第二封邮件里写到“APT1 是合法的，”该邮件还给出一个

包含两部分钓鱼邮件攻击的详细信息。钓鱼邮件攻击者功过发送‘良性电子邮件’建立潜在受害者的信任，随后便发送恶意的内容模仿真正的会话。新的“双管猎枪”功能为 PhishMe 用户提供简单模仿、培养并追踪对这类多面复杂攻击的回应。“我们服务各个级别的用户。PhishMe 公司的双管猎枪方案针对那些已经成功培训员工识别低级攻击并想进一步提升员工对高级复杂攻击识别能力的企业设计。”希格比说。

PhishMe 公司简介

PhishMe 帮助各大企业提高其员工针对钓鱼邮件攻击、恶意软件及路过式攻击的应变能力。该公司提供的具体指标可以轻松地衡量企业在管理员工安全行为方面的进步程度。全球 140 个国家超过 350 万的个人接受 PhishMe 方案的培训，已降低员工沦为高级网络攻击受害者的比率达到 80%。

PhishMe 公司方案定期对员工进行钓鱼场景模拟，并立即对发现的敏感对象进行培训。该解决方案针对用户行为提供清晰并准确的报告，允许用户衡量自身随时间推移的进步情况。PhishMe 公司与联邦机构和全球 1000 强公司合作，包括金融服务、医疗保健、高等教育和防御行业等。更多详细信息，见 www.phishme.com 。