网络钓鱼揭秘：钓鱼者的三种典型攻击手段

在大多数人的印象中，网络钓鱼就是那些欺骗人们提供银行账户或身份信息的假冒电子邮件。然而，据蜜网项目组&蜜网研究联盟（Honeynet Project & Research Alliance）最近发表的研究报告显示，网络钓鱼要比这更复杂和更可怕。

该联盟在这份最新的研究报告中警告说，网络钓鱼者正在使用恶意的网络服务器、端口重新定向和成功率相当高的蜜网诱骗用户上钩。他们的努力比人们最初想象的更周密而且更有组织性。在许多情况下，他们与其他的钓鱼团伙协调作业并且同时采用多种手段。

蜜网研究人员 Arthur Clune 在谈到这篇报告中的一个攻击的例子时说，这种钓鱼网站的建立速度是非常快的。所有这些网站都是事先准备好的。建立这种网站的人显然已经做好了准备，因为在这个网站还没有完全建好之前我们就开始看到有网络通信了。包括扫描有漏洞的网络服务器等活动在内所有的过程都是高度自动化的。这一切都表明，攻击者是认真的、做好准备的并且要尽可能多地寻找有漏洞的主机。

Clune 说，这类网站的质量和滥发邮件的做法正在改善。这类网站使用更规范的英语并且嵌入了质量更好的图片，使之在外表上更像是真正的网站。另一位研究人员 David Watson 则说，随着用户越来越了解网络钓鱼以及网络钓鱼的手段，攻击者不得不改进他们的方法。他说，受到这种攻击的人数之多使他感到意外。

Watson 说，在我们调查的许多诈骗事件中，我们吃惊地发现，用户确实会访问那些假冒的钓鱼网站。指导如何安全使用互联网的信息显然没有普及到最终用户。

这项研究是使用蜜罐进行的。所谓蜜罐指故意设置为没有保护措施的计算机。当受到攻击时，研究人员可以对这些攻击进行研究，更好地了解攻击者使用的策略。在蜜罐上，研究人员清楚的观察到钓鱼者成功地使用了三种不同的攻击手段：

攻破网络服务器

第一种方法是攻破有安全漏洞的服务器并且安装恶意的网页内容。在一次典型的钓鱼攻击中，攻击者使用了如下方法：

·扫描有安全漏洞的服务器；

·攻破有漏洞的服务器并且安装一个工具集或者口令保护后门；

·通过加密的后门进入那台被攻破的服务器；

·下载事先制作好的钓鱼网站，防止被攻破的服务器是基于网络的服务器；

·进行有限的内容配置和网站测试，当首次访问这个网站服务器时有可能会暴露他们真正的 IP 地址；

·下载大量发送电子邮件的工具，使用这种工具利用垃圾电子邮件为这个假冒的网站做广告；

·通过上述步骤之后，开始有人访问这个钓鱼网站，并且潜在的受害者开始访问这个网站的内容。

这个联盟在声明中说，从系统首次连接到互联网算起，这种攻击通常只有几个小时或者几天的时间。研究发现，攻击者经常是对许多台服务器和许多机构同时发起攻击。

端口重新定向

这是第二种攻击方法。据称，2005 年 1 月 11 日，一个攻击者利用 Redhat Linux 7.3 系统的安全漏洞成功地进入了一个蜜罐。

研究人员称，这个攻击事件有点不同寻常。攻击者突破了服务器之后并没有直接上载钓鱼的内容。取而代之的是攻击者在蜜罐中安装并且配置了一个端口重新定向服务。这个端口重新定向服务旨在把发送到蜜罐网络服务器的 HTTP 请求以透明的方式重新路由到另外一台远程服务器，使人们很难跟踪内容来源的位置。

研究人员说，攻击者随后在蜜罐服务器中下载和安装一个名为“redir”的端口重新定向工具软件。这个工具软件旨在透明地把进入蜜罐服务器的 TCP 连接发送到一个远程主机。攻击者设置这个软件，以便把所有通过 TCP 80 端口进入蜜罐服务器的通信重新定向到在中国的一台远程网络服务器的 TCP 80 端口。

蜜网

这是第三种钓鱼攻击方法。在 2004 年 9 月至 2005 年 1 月期间，德国蜜网计划部署了一系列没有使用补丁的基于 Windows 操作系统的蜜罐，以观察蜜网的活动情况。在此期间，发生了 100 多起单独的蜜网活动。

研究人员表示，他们捕获的某些版本的蜜罐软件能够远程启动在被攻破的服务器中的 SOCKS 代理。

研究报告则称，如果访问这个蜜网的攻击者能够启动远程蜜罐服务器中的 SOCKS 代理功能，这台服务器就能够被用来发送大量的垃圾电子邮件。如果一个蜜网包含大量的被攻破的主机，攻击者就可以非常容易地从毫不察觉的家庭电脑用户拥有的大量的 IP 地址发送大量的电子邮件。

资源丰富的蜜网的拥有者利用蜜网从事犯罪活动也许不会使人们感到意外。现在是租用蜜网的时候了。蜜网的经营者将向客户出售具有 SOCKS v4 功能的服务器 IP 地址和端口的列表。有很多文件证明，有人把蜜网出售给垃圾邮件制造者作为转发垃圾邮件的工具。

底线

在挑选了上述这些攻击方法之后，研究人员做出结论称，钓鱼攻击能够很快地发生。从首次入侵服务器到在网络上建起钓鱼网站只需要非常短的时间。这就使网络钓鱼很难跟踪和预防。这篇研究报告显示，许多钓鱼攻击都是同时采取多种手段、组织得非常复杂并且经常联合采用上面介绍的手段。

IT 管理员应该做什么？

Watson 指出，黑客经常扫描大量的 IP 地址，寻找可以攻击的有漏洞的主机。这种扫描活动是不分青红皂白的。漏洞最多的服务器将首先被黑客找到。因此，网络管理员要采取最佳的安全做法并且修复系统的安全漏洞，使用防火墙并且执行严格的身份识别措施，或者封锁不必要的进入服务器的连接。

蜜网研究人员 Clune 赞同这个观点，并且对 IT 管理员提出如下建议：

1）提高警惕。钓鱼网站从建立到开始活动是很快的。这些人预计这种钓鱼网站存在时间很短，因此，需要建立很多这类网站。钓鱼网站虽然存在的时间短，但是，在被发现之前造成的损失是很大的，特别是在周末。

2）对简单的事情也要加小心。阻止直接发出的简单邮件传输协议进入你所有的机器以及进入服务器的 HTTP/HTTPS 请求等简单的事情使你的服务器不容易被黑客利用，从而使黑客转向其它容易利用的服务器。通过你的网关强制

执行简单邮件传输协议并且同时运行查找垃圾邮件的软件可能会完全阻止你的服务器发送垃圾电子邮件。从信誉的角度说，这是一种很好的方法