访问路径检测的网络防御新技术①

何昱阳

(汕头职业技术学院，汕头 515078)

摘 要：针对防火墙、入侵检测等网络防御技术的不足，通过近几年的分析研究，本文提出一种访问路径检测的网络防御新技术，可以较好地预防网络钓鱼和木马盗出数据。

关键词：访问路径检测；网络防御；新技术；网络钓鱼；木马

Network Defense New Technique of the Visit Path Examination

HE Han-Yang

(Shantou Polytechnic, Shantou 515078, China)

Abstract：Due to the firewall and IDS etc. the network defendoof technical shortage, Pass the last few years of analysis research, this paper puts forward a kind of according to visit path examination of network defense new technique, can a little bit well prevent network from going fishing with the trojan horse steals user's datas.

Key words：visit path examination; network defense; new technique; phishing; trojan horse

在现有的网络防御技术中，主要有防火墙技术、入侵检测和防御技术，这些技术各有其优缺点，对于技术高超的木马，其防御性能仍然力不从心。例如，在网银账号被盗案例中，黑客通过向用户计算机中植入木马，远程收集用户的账号、密码贩卖给不法分子，造成网银用户资金莫名奇妙地丢失。笔者通过长期对这些技术的跟踪和分析，提出一种基于访问路径检测的网络防御技术，经过近几年的测试、改进，取得了较好的防御效果。

1 访问路径检测的基本原理

目前，网络受攻击的方法有很多，但从攻击的途径来看，大概就是两种[1-2]：其一是外部直接攻击，主要通过网络扫描、监听，发现系统漏洞，或者通过伪造 IP 包进行 WWW 欺骗、网页钓鱼，从而非法获取用户账号密码及系统特权。其二，攻击者通过在用户系统内放置木马，来非法获得相关信息。

对于第一种情况，防火墙技术和入侵检测技术可以进行一定程度上有效的防御，但对 IP 包欺骗和网页钓鱼是不能有效防御。对于第二种情况，通过杀毒软件和防火墙过滤技术，可以有限度地进行防御，但对那些技术高超的木马似乎力不从心。有时当人们连上网络，进行网上冲浪时，这些隐藏很深的木马，在偷偷地把你的重要资料发往远程某个主机，近年轰动一时的网银账号被盗案，就是这种木马所为。

在上网时，我们担心接收来历不明的 IP 数据包，但更忧虑自己的机器向外自动发送自己不知道的信息，这正是本文要讨论的问题。根据 IP 协议原理，在浏览网页时，IP 数据包一般只是在本地主机和目标主机及 DNS 主机之间流动，对于 DNS 主机一般情况下是安全的，如果能检测到目标主机是正确的，与所访问的网页的 IP 地址相符，那就可以确定本次访问是安全的；如果网络流中 IP 包地址与本机 IP 及目标主机的 IP 不符，就提出警告，提示用户是否进行拦截。这就是访问路径检测的网络防御基本原理。

这个方法能有效地防御网络钓鱼，并能很好地防止本机数据不明流出，使我们在访问网络时，能清楚和放心本机流进及流出的数据。

① 收稿时间:2011-09-08;收到修改稿时间:2011-10-17

2　系统设计概述

访问路径检测技术就是检测浏览器访问的路径是否是正确的。一般人们打开浏览器访问网络站点时，通常有可能打开几个或更多的页面，但在同一时刻，活动的页面(Active WebPage)只有一个，将这些页面的标题和 URL 送到系统数据队列，通过访问路径的综合统计分析，并与从 Socket 中实时获取流进流出 IP 包的目标地址进行比对，从而确定 Active WebPage 的目标地址是否正确，若有差异，系统就发出警告，提示用户是否要拦截，还是继续，软件系统设计的原理如下图 1 所示。

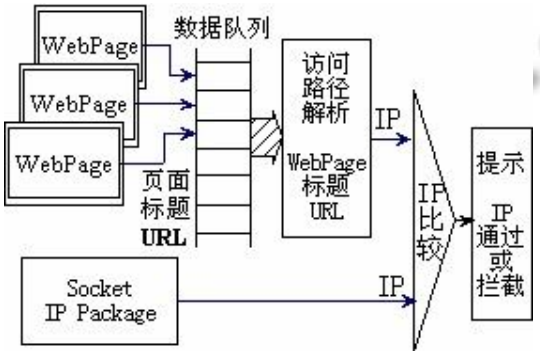

图 1　系统设计原理图

3　系统设计的关键问题分析

系统设计的关键问题有如下几点：

第一，访问路径解析及期望 IP 地址确定，这是软件系统设计的重点和难点。如何确定 Active WebPage 是否是用户所访问的真实页面，而不是钓鱼网页？到目前为止，这的确是个难题。笔者通过长期研究分析，认为较为折中的办法是通过 WebPage 标题和 URL 综合分析判定，来推断当前 WebPage 是否是真实页面。

图 2　WebPage 标题及 URL 综合分析

对于一些规范的网站（如网银、支付宝等），页面标题一般都有明确的站名标示，如图 2 中椭圆圈中所示，这样就可以根据站名标示反查其 IP 地址，与 IP 数据包中的目标地址比对，就可以发现当前 Active WebPage 是否是钓鱼页面。尽管钓鱼页面的标题可以与真实页面的标题做成一样，但其 IP 包的目标地址是绝对不同的。

然而，即使是正规的网站，不同的页面，其页面标题中站名标示也不尽相同，有些有，有些没有，或者站名标示不统一，这时只能分析其 URL 了。如图 2 中长方形圈中所示，提取 URL 中的关键域名字段，进入软件系统的数据队列进行分析。一般来说，钓鱼页面总是瞬间到来的，其域名可以做得与真实页面的 URL 相似，但毕竟是不同的。再通过用户访问路径的连续性进行综合分析，可以较高程度地发现钓鱼页面。这其中的算法分析较复杂，限于篇幅，这里就不讨论了。

为了提高系统的防御应对速度和防御效果，对于用户重要页面，如网银、支付宝等，在系统内部可以先建立特征库，同时对访问的页面处理可分为几个等级，以简化算法分析的难度，提高系统的响应时间。

第二，WebPage 标题及 URL 反解析问题。有些域名或路径是不能解析出 IP 地址的，并且反查 IP 地址的时间较长，为了提升系统的反应时间，系统中自设 IP 地址反查模块，类似 114best.com 系统，在系统联网时可以自动更新数据。该模块还能查出 IP 所属地域及单位名称，以提交用户进行实时分析决策。

第三，预防木马在后台偷偷发送数据，这个问题的解决相对容易一些。一般来说，网络中的 IP 数据包在本机与 DNS 服务器及目标服务器之间流动，目标服务器的地址就是用户所打开的网页地址，并存放在系统数据队列中，实时检测流出本机 IP 数据包的目标地址，如果不在数据队列的范围中，系统就发出警告，提示用户是否拦截。若用户有 QQ、MSN 这类软件加载，可以把其服务器地址添加到数据队列中。

4　使用效果分析

该软件系统在实际过程中，其网络防御作用是很明显的。例如，在访问“淘宝网”时，让系统进入“特护”模式，为了减少干扰，用户打开的页面只有“淘宝”网和“支付宝”网，这样一旦出现钓鱼页面，其

防御效果非常理想。

如图 3 所示，钓鱼页面与支付宝的真实页面非常相似，肉眼很难分辨真假。图中椭圆圈中的部分，URL 地址是 a1ipay.com，不是“支付宝”的域名 alipay.com，前者是数字 1，后者是英文字母 l。

图 3 在访问“支付宝”时出现的钓鱼页面

上述情况的钓鱼页面是自设软件产生的实验结果，通过多次实验分析，在“特护”模式中，防御网络钓鱼的准确率可达到百分之百。

在预防木马在后台偷偷向未知站点发送数据的测试中，实验效果也很理想。不管木马是通过中间代理站点，还是直接向最终站点发送[3]，只要 IP 包目标地址在用户访问路径数据队列中不存在，系统就发出警报，提示拦截或是放行，如图 4 所示。

图 4 在浏览 CSDN.NET 网站时用户机器在后台偷偷发送数据

在这种情况中，如果木马以中间代理站点或最终站点的 URL 偷偷打开一个页面，那这种方法会存在漏检现象，因此用户在使用中不要打开过多的浏览器窗口，没用的要及时关闭，同时立即关闭那些自动弹出的页面。

5 结语

在目前众多的网络防御方法中，访问路径检测技术是一种较新颖的防御技术，在目前网络钓鱼，木马泛滥的网络环境中，对保护用户的账号和密码、以及用户本机数据安全，能起到一定的作用。经过近几年的测试，访问路径检测技术经过不断的修改、完善，达到了初步的防御效果，可以使用户在访问网络时，不担心被钓鱼网页欺骗，不担心本机数据被偷偷地流出到某个不明站点，做到明白放心上网。

由于目前互联网的环境非常复杂，网站的制作水平差异和不规范统一，这对访问路径检测的正确性增添了极大的难度。如果互联网管理部门要求每个入网的网站的每个页面，在标题栏在开始处明确地标示出自己的站名，如图 3 和图 4 中所示的标题那样，访问路径检测技术将会取得非常好的效果。

参考文献

1 王宇,卢昱.基于访问路径的网络安全脆弱性分析.计算机应用研究,2008,25(6):1796–1798.

2 吴坤鸿,舒辉, 董卫宇.内核脱钩技术在检测 rootkit 木马信息隐藏中的应用.计算机工程与设计.2008,29(14):3635–3637.

3 闫巧,吴建平,江勇.网络攻击源追踪技术的分类和展望.清华大学学报(自然科学版).2005,45(4):497–500.