网页木马机理与防御方法研究

文/曾泽军

摘要

随着现代计算机网络的不断普及，网络安全问题越来越受到社会各界的重视。网页木马具有强大的远程控制作用，给用户的网络安全带来了巨大的隐患。本研究就网页木马的机理和和特点入手，对如何进行木马的防御进行简要的探讨，以提高网络应用的安全。

【关键词】网页木马 机理 防御方法

网页木马是一种以特定的页面元素作为攻击对象，利用浏览器及插件中的漏洞，在用户的服务器终端进行攻击和控制的程序。网页木马制作简单、传播速度快，而且破坏力强，能够隐蔽的将恶意的程序植入在用户的客户端，给用户的电脑软件造成破坏，危害用户的信息安全。近年来，研究者针对网页木马的机理和防御做了很多的研究，现总结如下。

1 网页木马的定义

网页木马的本质是一组恶意的网页代码。黑客通过在特定的网页或者系统中进行木马程序的植入。在用户下载或者执行包含的恶意文件时，隐藏的木马程序通过计算机的漏洞侵入到客户端的计算机中，远程控制客户端的资源。通过修改客户端的文件、下载用户的文件或者随意的客户端的计算机注册表和系统文件，窃取对方的计算机信息资料，甚至造成对方计算机的瘫痪。

一般情况下，网页木马表现为一组相互之间有链接关系的、含有恶意的程序代码的网页界面。相比于蠕虫等传统的具有自我复制功能的网络病毒，网页木马还可以在的终端端对用户的网页进行实时的控制，而且这种攻击方式对于防火墙的检测来说不易发现，可以有效地在用户的电脑中顺利进行恶意代码的植入，盗取个人信息和破坏电脑程序更加的方便。而且由于现代网络的普及，黑客可以利用网页木马进行盗用股票账号、信用卡账号等，以此来获取经济利益。因此，现代网页木马的危害性更大。

2 网页木马的工作原理

现代网页木马在进行网页侵入的时候，通常是采用一种被动攻击的模式。一般是根据某个浏览器或者电脑的插件的具体的常见漏洞而开发的，黑客将网页木马设置在服务器的终端，并事先对攻击的页面进行设定。当用户发起特定的网页访问请求的时候，网页木马的服务器对用户的行为作出回应，将包含木马的页面内容发送到用户的客户端。一旦发送成功，隐藏的木马页面被浏览器加载，而其中的特定程序在浏览器中被执行并通过利用电脑程序的漏洞进行下载、安装、执行某些恶意程序。由此可见，网页木马的特点是隐蔽性，可以在不知不觉中对用户的电脑程序造成影响。其安装时被动式的，但是可以有效地对抗电脑的防火墙，对于用户来说很难防范。

通常情况下，木马的攻击步骤包括以下几个方面：首先是木马的植入，木马程序在客户端电脑植入后，能够自动的进行程序的启动哈运行，对目标主机进行实施的控制。在此过程中，可以修改系统的文件，实现文件的自动加载；修改计算机系统的注册表，以掌握计算机的核心配置文件；或者对系统进行服务程序的添加，导致只要系统启动，就会运行木马的现象；修改文件的关联属性，导致文件的运行与木马的运行同步；此外还可以利用程序的自动运行的一些程序，实现自动化的运行，对系统的 DLL 进行更改等。其次，是由于木马的隐藏功能对计算机用户造成的危害，木马可以将其程序注册为服务，进行深度的隐藏；还可以使用可变的高端口或者系统的服务端口，进行有效的隐藏。在此，木马程序具有的监控技术。可以实现对客户机器的信息窃取，对用户的实践进行记录以及远程的进行目标机器的鼠标和键盘的管理和控制，对于客户端用户来说危害极大。

3 网页木马的漏洞利用机理

前面提到网页木马主要是通过用户的客户端浏览器或者插件的漏洞以实现对电脑的入侵的。在相应的漏洞下，绕过网络的防火墙，获得一定的执行权限，以实现恶意程序的下载与执行的最终目的。现阶段，网页木马多采用的 Java Script 脚本语言进行编写，一般情况下电脑的浏览器可以为此种语言与相关插件（API）之间的交互作用提供便利，网页木马程序可以很方便的通过调用其中的不安全语言编程，导致插件出现漏洞。而且，黑客也可以通过对脚本进行灵活的运用，对反病毒引擎的安全检查进行混淆。因此，网页木马可以利用的程序漏洞主要有任意下载 的 API 类漏洞和内存破坏漏洞。

前者主要存在与一些浏览器的插件中，很多浏览器中通常都会存在一些用来下载、上传、等功能的插件。而插件在安装的过程中，通常不受到重视。如果在 API 中未进行安全检查，就会存在网页木马进行直接的利用的危险。

后者主要主要分为是三种，分别为 use-after-free 型漏洞、溢出漏洞和浏览器解析漏洞三种。网页木马可以利用 Java Script, Vb Script 脚本向存在漏洞的浏览器内存中进行恶意的传输一些执行指令，导致相应的执行流跳转被触发，在控制下相应的程序进行下载和执行恶意的程序。

4 网页木马的防御方法

4.1 木马检测

首先是在日常使用电脑的过程中，尤其是进行文件的下载过程中，应该注意木马的监测。常见的检测方法有端口的扫描，对系统的进程进行检查以及对 .ini 文件、计算机的注册表以及服务进行经常的检查，或者对网络的通讯设备进行检查，通过定期的检查可以及时的发现木马，防止电脑被网页木马侵入，降低用户的损失。

4.2 木马的清除

一旦在电脑中发现木马的侵入，我们应该明确木马的加载部位及时的清除木马的登记部位，切断木马开机启动的功能。但是有些木马侵入的计算机注册变，会出现自动恢复的现象，因此操作者应该实现停止木马程序后再进行删除的操作。但是，目前的木马种类众多，攻击性和隐藏性越来越强，为了实现有效地查杀，还要借助专业的杀毒软件进行清除。

4.3 木马的防范

木马的防范应该从多方面入手，全面提高计算机的安全性。首先应该对计算机的漏洞进行及时的修补，安装补丁，防止被恶意的程序利用。其次，我们可以采用反病毒软件对程序进行实时的监控，经常进行软件的更新，下载专门的木马清除软件，对电脑进行木马的清除。再者用户应该增强防范意识，不随意下载软件，尤其是不规范网站的软件，最后，现阶段提出的基于网站服务器端进行网页挂马的防范，也是一个非常有效的方法。

综上所述，为了更好的使用计算机为我们的生活服务，我们应该了解网页木马的危害，及时的进行检测、防范和清除，杜绝网页木马的出现，提高信息的安全性。

参考文献

[1] 张慧琳，邹维，韩心慧．网页木马机理与防御技术 [J]．软件学报，2013, 04: 843-858.

[2] 郑云鹏．网页木马机理与防范对策 [J]．电子技术与软件工程，2014, 12: 233.

作者单位

1. 上海同济大学软件学院　上海市　200096

2. 内蒙古集宁师范学院　内蒙古自治区乌兰察布市　012000