计算机木马的社会化和防御体系

■ 广东金融学院 赖瑞麟

摘 要 :当前网络中蕴藏了越来越多的企业财富和个人财产，这给以窃取资金为目的的木马病毒巨大的发展动力，木马盗窃形成“ 流程化 ”和“ 产业化 ”，他们编写木马，传播木马，盗取网络财产，然后由第三方销赃。本文从木马的社会危害切入，结合木马的入侵预防手段和木马“ 云安全 ”防御体系，来剖析对付木马的最佳办法。

关键词 :科技 ;木马 ;注册表 ;入侵 ;扫描引擎 ;云安全

一、介绍

木马由2部分组成，服务器（受害计算机）和客户端（黑客计算机）。当木马入侵到受害计算机后，和客户端网络连接，黑客通过控制程序发出命令，木马在服务器上执行任意的操作，如截取屏幕、搜索账号密码、记录键盘敲击等，最后把用户私人信息发送给客户端。

木马这种以盗窃信息为目的病毒在当今网络时代充当了主要的作案工具。无论是网银中真实的钱，还是虚拟财产，都成为了木马盗窃的对象。

二、木马的社会危害

(一) 木马“ 流程化 ”

在黑客网站，整套木马攻击手段被广泛流传，攻击者把木马的攻击流程完全“ 自动化 ”。安装控制端、扫描端口、远程植入、上传下载账号密码构成了木马盗窃一条龙。黑客宣称，木马攻击的成功率仅取决于黑客计算机性能和网络带宽。

(二) 木马“ 产业化 ”

木马已经形成“ 产供销 ”的黑色产业链。在链中的最高层是木马程序员，他们称为“ 造枪的 ”。木马会被出售给零售商，称之为“ 卖枪的 ”。“ 卖枪的 ”通过自建网站，向盗窃实施者销售木马。这些人就是“ 拿箱子的 ”。盗窃实施者雇佣散工，称为“ 挂马的 ”，把木马广泛传播。当木马在受害者计算机“ 肉鸡 ”运行后，“ 拿箱子的 ”会收集海量的包含账号密码的电子邮件。

这时“ 拿箱子的 ”会把账号密码打包转卖给“ 大买家 ”，或者自行洗劫。例如游戏中某虚拟物品，从“ 肉鸡 ”账号中盗窃出来后，转移到一个仓库账号，再兑换成容易流通的虚拟物品，并在淘宝等平台以低廉的价格拍卖出售。这样的产业化环环相扣，从一连串代码变成各个阶段的真金白银。

三、木马的防治策略

木马防治策略，应以预防入侵为主，及时升级杀毒软件、实时监控软件和防火墙为辅助，加入“ 云安全 ”体系为主要防治手段。

(一) 防治木马入侵

木马对计算机的影响行为有 :木马植入、自动启动、隐藏和远程控制。作为木马登陆本地的第一环节，如果能事先把木马成功拦截在本地之外，黑客木马将无从施展。

以下从木马的非法入侵的4个途径来剖析入侵原理和对付方法。

1. 移动存储器式入侵

当用户插入带毒的可移动磁盘时，盘内的Autorun.inf会自动运行，把木马植入到本地，例如“ Auto病毒 ”。

其防治方法很简单，当插入移动存储器后，先利用反毒软件进行扫描，确保无毒后才用鼠标右键打开磁

盘。另外也可把注册表中HKEY_CURREN_USER主键下的“ NoDriveTypeAutoRun ”项设置为“ F6000000 ”，那就关闭了光盘和U盘的自动运行功能。

2. 电子邮件入侵

当用户粗心地下载了带毒电子邮件中的附件（通常格式为VBS，SHS等），无论是否运行，也会立刻感染木马病毒。

虽然现在大型的邮件服务器都有过滤功能，但对于新型的木马，还要养成良好的防毒习惯。不要打开来历不明的邮件，即使是熟悉的人发来的邮件，如果题目混乱，可以认为是木马。即使下载了邮件附件，也应该立即扫描查杀毒。

3. 网页挂马入侵

当用户访问非法网站，IE在后台会运行ActiveX脚本语言，这样木马就会成功地进入本地系统。

防治方法是，运行services.msc命令，禁止WSH（windows scripting host）服务。并且在IE选项中，禁止执行一切关于ActiveX的脚本。但是如此操作也会使原本丰富多彩的网页失去光彩。

4. 网络扫描入侵

黑客使用购买的扫描引擎发现开放端口的计算机，接着利用“ 种植者 ”等黑客工具，攻击这些有漏洞的“ 肉鸡 ”；在成功获取远程计算机的管理权限后，把木马下载到“ 肉鸡 ”中。

Windows防火墙对不断更新的木马是完全没有抵抗能力的，而安装防毒厂商的防火墙则是最佳选择，如金山网镖、瑞星防火墙、天网等。

（二）“ 云安全 ”防御体系

1. 什么是“ 云安全 ”

除了在计算机系统外拦截木马，还可以加入到“ 云安全 ”防御体系。“ 云安全 ”即安全的互联网化，是通过分布式的客户端对网上程序行为进行监测，获取异常的木马、病毒，发送到服务器端进行虚拟机分析和服务器处理，再把解决方案更新到每个客户端。

2. “ 云安全 ”的行为

“ 云安全 ”系统包括客户端和“ 云安全 ”中心。以瑞星“ 云安全 ”为例，“ 云安全 ”客户端就是安装了瑞星软件或者某些网络软件的计算机。这些网络软件厂商都加入了“ 云安全 ”计划，如百度、迅雷等。“ 云安全 ”计划中的网络软件组成了“ 云安全探针 ”（如瑞星2012、快车、电驴等）。“ 云安全探针 ”对网络上的异常

行为和本地计算机安全信息进行探测，如邮件服务器上的带毒邮件、搜索引擎中的木马网站、木马对系统注册表修改的行为等。

“ 云安全 ”中心由威胁信息数据中心、威胁信息分析服务器、挖掘服务器和升级服务器等组成。

当新木马信息被“ 云安全探针 ”捕获后，立即发送到威胁信息数据中心，由威胁信息分析服务器进行分析，形成一个解决方案。然后上传到升级服务器中，通知“ 云安全探针 ”下载更新。同时，挖掘服务器群会挖掘这些可疑木马的来源。当定位到带毒网页后，“ 云安全 ”系统会将网址发送给合作伙伴，搜索引擎、下载软件等将第一时间屏蔽带毒网站。

四、结束语

木马是当前网络信息化的产物，木马犯罪是对网络财产的盗窃行为。面对层出不穷的木马技术和违法手段，冷静分析其运行原理和幕后操控，不仅是网络安全厂商，还是网络执法人员必须具备的素质。文本仅从木马的事先预防和当前卓有成效“ 云安全 ”体系讨论，希望读者可以从文中得到一点共鸣。FTT

参考文献：

[1]瑞星公司.瑞星“ 云安全“ 发展历程[DB/oL].http://www.rising.com.cn/2009/cs2010/course.html

[2]林洁.浅议注册表在反计算机病毒中的作用[J].中国高新技术企业，2008，4.

[3]刘申晓.浅谈计算机木马病毒的解析与防范[J].福建电脑，2011，3.