

后病毒时代到来,“绿化”E生活迫在眉睫

木马肆虐,你我“很受伤”

■事件

市民晓庆是刚投身股市的新股民,近日,当她像往常一样在网上打开自己的交易账户时,发现的一切让她迷惑不已,“2000股万科在震荡时被低价抛了,我记得自己没卖啊!而上海医药和*ST宝硕两只股票,不知道怎么就买进了?”朋友告诉晓庆,她很可能是中了一“证券大盗”的木马,黑客利用这一恶意程序窃得了她的交易账户,随后将其股票低卖高买的。

据统计,从2004年8月到2007年6月,全国感染各类网银木马及其变种的用户数量增长了600多倍,而且其发展正在呈加速上升趋势,通过木马窃取QQ密码、网游账户、电子支付口令、电子邮件账号等的案例更是不胜枚举。专家表示,相比普通病毒,木马往往以盗窃、诈骗钱财为目的,且具有更强的隐蔽性、传播性,难以查杀,其危害远远超过了普通病毒,已经成为了互联网安全的最大隐患。

本组撰稿 快报记者徐勇

木马背后 藏有灰色产业链

“互联网是现实社会的缩影,当网络犯罪者们开始发现‘蠕虫’或者普通病毒并不能过多地为自己带来商业回报,于是纷纷将‘研发’的重心转向了更有‘钱途’的木马程序。”江苏省内一位互联网专家表示,木马横行以及它对利益诉求的背后,是一大批从业者及辅助平台的存在。“这一行利润丰厚,足够支撑起一条完整的产业链。”

据知情人士透露,不管是网银中真实的钱,还是虚拟物品,制造木马、传播木马、盗窃账户信息、第三方平台销赃、洗钱,是普遍采取的流程。以这段时间炒得沸沸扬扬的“证券大盗”木马为例,木马的制造者本身并不参与“赚钱”,病毒编写完毕后,大量的“大虾”开始招募“徒弟”,教授木马病毒控制技术和盗号技术,收取“培训费”,之后往往将“徒弟”发展为下线(也就是其代理商或分销商),以辅助完成其他牟利活动。

许多迹象表明,黑客不再是单机时代那个“拿弹弓打邻居玻璃”的顽童形象了,撰写病毒也不再是他们的乐趣,或者炫耀技术的方式。在互联网蓬勃发展的今天,这已经成

为敛财的捷径。“木马产业链就像一只精密的瑞士手表,一环扣一环,有序地运转着。上家与下家互相依赖,互相博弈,虽有摩擦,但彼此依然为共同的利益推动着这份‘朝阳产业’。”一位业内人士这样形容。

木马危害 远基于普通病毒

除了趋利性,从安全角度来看,木马也已经“异军突起”,成为后病毒时代的“毒王”。

瑞星公司防病毒专家史■表示,木马一般并不像普通病毒那样具备复制功能,并不主动去感染其他软件,但它可以通过“网站挂马”、文件传输、移动介质(如U盘)等各种隐蔽的形式,大面积传播感染用户电脑,“这种不易察觉的隐蔽性往往比病毒还凶猛。”

而且正是因为木马可以长期潜伏在用户系统中,发作前并无明显征兆,其隐蔽性强的特点让它更容易逃过病毒检测,也容易被用户忽视。”史■进一步表示。

此外,从Google调研全球数以十亿计的网站中抽取的450万个网页的分析测试中发现,至少有45万个页面中含有恶意脚本。而最近疯狂肆虐的“德夫下载器”木马病毒,在自身传播的同时可下载并执行其他11个盗号木马,从魔兽世界、征途到武林外传

等11款网络游戏都难幸免。

更为糟糕的是,目前不少网银系统中所存在的安全隐患,给木马“钓鱼网站”留下了可趁之机,这也让许多用户为之担心不已。

■专家指点

提防木马 提升免疫重在防御

“木马病毒肆意横行且发展迅猛,而与之相对的木马查杀市场也同样得到了高度重视。”瑞星安全专家表示,目前网民对木马的查杀可以通过杀毒软件中集成的木马查杀功能、防火墙中集成的木马拦截功能来进行,对于没有安全杀毒软件的电脑用户,也可以下载瑞星提供相应的专杀工具;诺顿、金山、江民等杀毒软件公司也同样表示,他们对诸多木马同样有防御与查杀的功能。此外,据业内人士介绍,一些辅助软件譬如“360安全卫士”,对木马的免疫、查杀、防御表现得也很有优势。

“免疫功能让你的电脑增强抵抗力,木马难以入侵,系统漏洞自动回复、IE防漏墙技术、U盘病毒免疫等功能对木马还是非常奏效的”,多位信息安全专家表示,提防或避免木马还是要重在预防,安装杀毒软件的用户要及时地升级并更新病毒库与防火墙,已中了相关木马的电脑用户不防选择较合适的查杀工具来去除木马带来的危害。

我的数码时尚生活 BenQ

Follow Me 做超级玩家

“游戏狂人”王勤在领到参加工作的第一份工资后,就送给自己BenQ Joyhub NASA台式电脑,“有一次在电脑城看到有人用NASA配合游戏方向盘极品飞车,就再也忍不住了!”酷炫3C品牌BenQ,特别为年轻一族量身定制了极具战斗力的Joyhub NASA,以创新外观设计、显示技术、强劲游戏功能,带来视、触、听全方位游戏盛宴。



Joyhub NASA 搭配发烧级19英寸/24英寸大屏BenQ钢弹系列液晶显示器;16:10宽屏,带来强大视觉冲击;Senseye+game显彩2代技术,提供两种特设游戏模式(竞速/动作),并针对不同色彩信号进行独立调整,让暗部细节清晰、色彩鲜活。NASA显示效果极佳,不论亮处或暗处,都呈现高质量画面。对于Quake3这类射击游戏,Joyhub NASA灰阶2毫秒极速响应时间。此外,Joyhub NASA还采用支持DVI数字接口的独立显卡,保证高质量的图像传播。

NASA符合人体工学设计的X架构键盘带来琴键般触感,鼠标也舒适顺手。“无论跳舞毯等完全依靠键盘敲击的游戏,还是需键盘鼠标充分配合的射击枪战类游戏,Joyhub NASA键鼠带来的使用感受都不错。”听觉方面,NASA配备2.1全木质音箱,“空间定位能力明显,细节处还原真实细腻,高音部分悠扬婉转,低音也处理得雄厚纯正。”王勤兴奋地说,“这个夏季,Follow Me,让我们转战新‘战场’,尽情火拼吧!”

咨询热线:
13951687927 王先生
13601585454 姜先生

瑞星反病毒反木马一周播报: 新病毒劫持QQ乱发消息 盗取用户帐号(2007.06.25-07.01)

本周病毒:
QQ通行证变种 TNC (Trojan.PSW.QQPass.tnc)

警惕程度: ★★☆☆

它是一个能在WIN9X/NT/2000/XP系统上运行的蠕虫病毒。该病毒运行后会自动向用户好友的QQ发送内容为“这里有我的照片帮我顶下记得回复我哦哦点击就可下载”的消息,并附带一个网址。消息中的网址即为病毒链接,其他用户下载打开该文件就可能被病毒感染。该病毒会窃取用户的QQ账号,给用户带来损失。同时,它还试图通过优盘、移动硬盘等移动存储设备传播,一般用户很难手工将其删除。

专家建议:
1. 遇到好友通过QQ及MSN等工具发来的网址或文件时,应先和对方确认再

打开;2. 打开杀毒软件的实时监控程序,并关闭系统的“自动播放”功能,防止病毒通过优盘侵入电脑。

查杀方法:
请广大用户及时升级手中的瑞星杀毒软件2007版或下载到19.29及更高版本。没有安装杀毒软件的朋友可以登陆<http://online.rising.com.cn>使用瑞星在线杀毒清除病毒,同时可拨打反病毒急救电话010-82678800或登录<http://help.rising.com.cn>使用在线专家门诊免费寻求帮助。



M-zone 人吃定音乐!
动感地带音乐套餐全新上市

动感地带音乐套餐新鲜出炉。从此,音乐也是我的地盘。首发新歌,我先听;潮爆彩铃,酷炫手机音乐,想下就下。每月20元,包含150条点对点短信和梦网上行短信,彩铃功能费,无线音乐俱乐部高级会员功能费,10M GPRS流量和免费下载3条彩铃(登录www.12530.com即可轻松下载最新最酷的彩铃)。特权多多,优惠不断,好音乐,大小通吃。

详情请咨询当地10086

客户服务热线: **10086**
www.m-zone.com.cn