盗得两千多万个账号 非法获利数百万元

江苏破获全国首例木马病毒案

2008年7月中旬,经过4个多月的缜密侦查,盛名一时的“伯乐”木马制造者吉才在深圳被江苏扬州警方抓获,这一团伙苦心经营一年多的庞大“帝国”瞬间轰然倒塌,20多名主要犯罪嫌疑人落入法网。

“伯乐”不识马专门养“木马”

价值 8000 元“宝刀”被盗

今年 4 月初,网民小秋玩电脑游戏时,屏幕上突然跳出一个窗口,称点击下载该程序后,可以提高游戏运行速度,小秋丝毫没有犹豫,点了下去。

然而,时隔 10 分钟左右,许多莫名网站陆续弹出,且无法关掉,小秋估计可能中毒了,随即关闭电脑。可当他再次打开自己的游戏账号时,意外发生了:身上的装备全都蒸发,一把价值 8000 元的宝刀,也没有了踪影。

玩过网上游戏的人都知道,电脑游戏里的装备虽然是虚拟的,但都可以通过现金来确定价格并交易,小秋认为这是别人采取了非法的手段盗取了自己的游戏装备,便立即报警。

此时扬州市公安局网警支队十分忙碌。近期,通过互联网的报警处理平台每天接受这类游戏装备被盗案件十几起。

经查证,警方判断,这很可能是一种叫“伯乐”的木马病毒所为。

循着“蹄印”找到“养马人”

警方决定以此为突破口。在扬州市公安局网警支队里,数十台电脑前,民警查访各大游戏网站和论坛,通过对数万信息的筛选、研判,终于找到“马蹄印迹”,一个自称该款病毒制造者的人进入警方视线,他的网名就叫“伯乐”。

7 月 8 日,“捉马行动”全面展开。

当天上午,扬州火车站候车大厅内人来人往,喧闹嘈杂。一对年轻的夫妻正有说有笑地等待火车进站。“你好‘伯乐’,我们是警察,请跟我们走一趟。”年轻人周围突然出现一队警察,大厅内一阵骚动,随即沉静下来。妻子木然站立不知所措,男子知道事已败露,低声对警察说:“我跟你们走,只是请留点面子。”警察听出话外之音,未给他上手铐,只是警惕地站在他身边。男子神色黯然地牵着妻子的手,随警察离去。

在广陵公安分局,“伯乐”交代,木马程序的制作、销售是一个分工明确的组织,而他仅仅负责网上销售。所有的病毒程序都是一个叫“大哥”的男子提供的,由于只是网上交易,“大哥”姓什么,长什么样子一概不知。

在浙江发现病毒源代码

查看“伯乐”与“大哥”交谈记录,民警发现“大哥”来自浙江台州,且未察觉到“伯乐”已经落入警方之手。7 月 9 日,也就是“伯乐”落网的第二天,抓捕小分队出现在台州某小区。

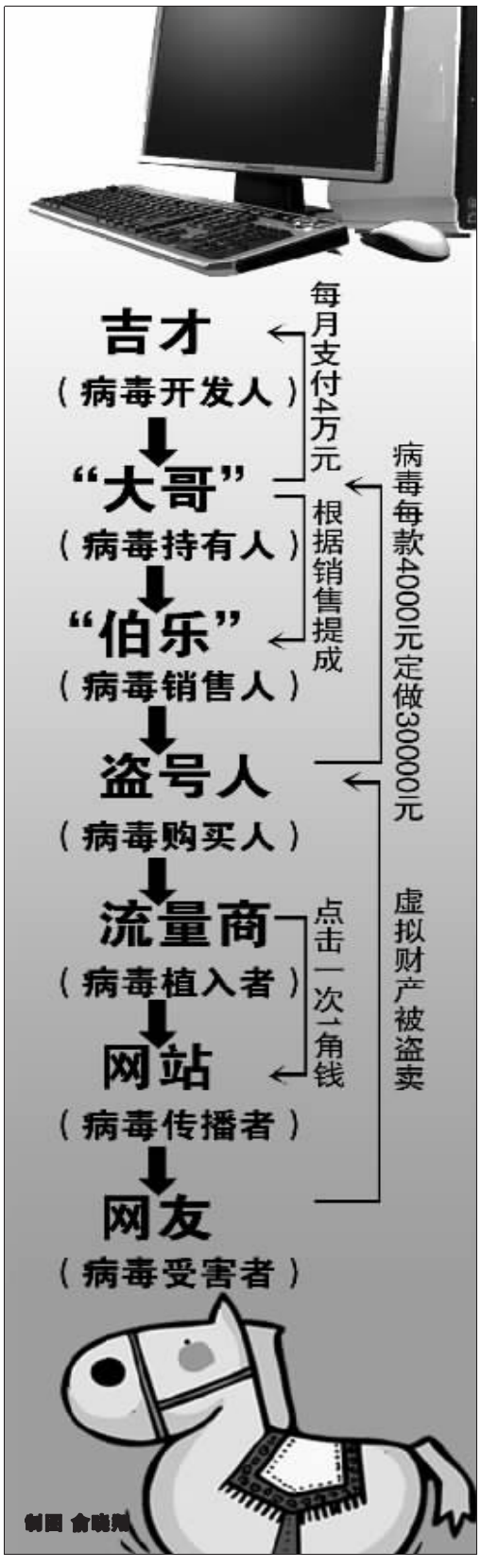
“你好,请开门,我们是小区物管。”民警按下门铃后大声说道。门打开一条缝,民警推门而入,将毫无准备的“大哥”抓获。民警环视左右,发现“大哥”的屋内装潢豪华,但却并不像一个制造病毒的工作室。疑惑之际,另一民警看出猫腻,此房是楼中楼,且经过伪装,需从外楼梯才能到达顶楼。打开楼上大门,场景令人震惊,10 多台台式电脑、笔记本电脑、服务器交错排开,4 名工作人员正在检测新编写的“伯乐”木马病毒。

在“大哥”的保险箱里,民警又有重大发现,这里不仅摆放了 130 多万元的存单,还有一个精致的移动硬盘。大哥交代,硬盘中存储的正是“伯乐”木马的源代码。就在民警欢欣鼓舞,认为已将这个团伙连根拔起的时候,一个令大家意想不到的结果出现了,“大哥”交代“伯乐”木马的编写者并不是他,而是另有其人,名叫吉才,居住在深圳。

7 月 14 日,吉才独自一人用餐,当他走出餐厅时,等候已久的民警将他带上车。经吉才交代,他确是伯乐木马病毒的始作俑者。吉才也成为全国首个被抓获的木马病毒制造者。

拔出萝卜带出泥,随后警方又马不停蹄上北京,下广州等地,行程数万公里,抓获涉案嫌疑人 20 多名,缴获赃款 200 多万元。

盗号黑色产业链



“病毒之父”只有初中文化

白白净净、年轻、头发微鬈,这是吉才留给人的第一印象,然而这个帅气的青年却是叱咤网络的“伯乐木马”的始作俑者。

吉才是湖南郴州人。据吉才说,初中时他的成绩在班上排名中游,毕业后就外出打工。2000 年左右,吉才来到郴州电脑城,第一次接触到电脑和网络,并被深深吸引。面对神奇的电脑,吉才突然来了学习兴趣,在初中文化的基础上,自学英语和数学,并开始学习编写小程序。

兴趣是最好的老师,扎进电脑知识的海洋,吉才如饥似渴,从早上起床到次日凌晨,他就像被粘在了电脑前的椅子上,动也不动。不久,吉才编写的 WINDOWS 操作系统维护程序诞生了,并由此引得郴州电脑、网络同行们的关注。

2002 年吉才来到深圳谋求进一步发展,并在某电脑公司从事编程工作,编程技术日益精进。行业内的人,经常找到吉才编写程序及相关模块。2007 年,吉才通过熟人介绍认识了“大哥”。此时,在网络里混了多年的“大哥”看准一个“商机”,即通过木马程序盗取游戏者的装备,再转卖给游戏者,以获取巨额利益。正需要金钱的吉才与“大哥”一拍即合。

据吉才交代,他负责编写、维护并升级木马程序,每月可从“大哥”处获得 4 万元的收入。编写一个木马病毒收益如此之大,财富从何而来?随着对涉案当事人审查的深入,一个庞大的黑色产业链条呈现在民警面前。

盗号黑色产业链浮出水面

要说清这个产业链并非易事,因为其结构过于庞杂,犹如一个树形结构,在主干上生出许多枝干,枝干上又长出许多枝丫。这里,我们以主干为表述核心进行解析。

如果把主干形容成一个公司,那么“大哥”就是公司老板;吉才是技术总监,负责产品制造与升级;“伯乐”是销售总监。

买主是那些专门从事盗号的人。每款木马的价格在 4000 元左右。如果买主要求单独为其制作一个木马,需要支付 30000 元左右的费用。另外,木马要不断升级以避免杀毒软件查杀,买家还得另外支付升级费用。

这些买主大多为盗号者,他们通过“流量商”将木马病毒植入他人的计算机内。由于“流量商”与许多网站都十分熟悉,并有业务往来,他们将已伪装成广告等形式的木马病毒,放到点击率较高的网站主网上,当你点击到那些弹出窗口时,木马病毒就“种”到了你的计算机上。

“流量商”按每次点击 1 角钱的价格,回报网站。据涉案人员交代,由于全国网民人数众多,他们每天能种 10 万多个“马”,为此也要支付万余元的费用。

“伯乐”交代,网友中毒后,当启动游戏时,自己的账号与密码就会自动出现在盗号者的眼前。面对如雪片般飞来的信息,盗号团伙一方面使用被盗网民的用户名密码登录游戏,清洗玩家的游戏币、装备等虚拟财产,然后通过专门的网络再在网上销售,从中赚取利润。

来不及处理的,就干脆再倒卖信件。据涉案人员交代,2007 年 12 月以来就通过传播“伯乐”等有害程序,盗窃游戏账号 2000 万余封,非法获利数百万元。

通讯员 扬公轩 快报记者 朱俊骏

毛发专家解读秋天脱发

头发大把大把地掉,不敢梳头,害怕洗澡,起床不堪回首,因为到处都会看到自己心爱的头发,大把大把的脱落,头发日渐稀少,真害怕照这样的速度脱下去,自己的头发挨不过今年的冬天,就会暴露头皮。真想知道如何才能快速停止脱发?

专家支招:秋天是脱发最严重的季节,头发大量的脱落是很普遍的,头皮本身属于亚健康的人士就要特别注意了,脱发人士经常因为不太在意而错过最佳止脱时机。尤其是平时头油多、头屑多等现象的脱发人士,这个时候的大把脱落很容易导致头发进入脱发急性期,不采取正确的手段结果将不堪设想,很可能在一两个月内就会露出头皮,那时就得需要漫长的恢复过程了。专家认为,秋天脱发可以通过章光 101 快速解决。

章光 101 为生发液剂,可以迅速渗透到毛囊的底部,活性因子不断激发刚刚脱落的发根,使其再次恢复生长机能,并有效激活毛母细胞,快速分裂形成新生发根,与此同时,生发液富含的毛发所需营养成分开始不断地输送给新生发根,使发根可以加快生长速度。

江苏省各地区均有章光 101 服务中心专业人员为您解决脱发问题。详细地址请致电:025-52335101