顶尖黑客写出“免杀”木马程序 7个下家组团狂盗游戏账号卖钱

关押期间这个黑客帮警方破过要案，公诉方建议处3到7年有期徒刑

80后、非常优秀的计算机程序员、在国内外黑客界很有名……拥有这些标签的罗华，本不该为钱发愁，可他禁不住诱惑，为别人编写并维护木马程序。下家买来程序后，用于盗窃游戏玩家的账号和密码。

昨天，南京下关法院开庭审理了这起案件，罗华等两人被指控涉嫌提供侵入计算机信息系统程序罪，专门盗号的7名下家被指控非法获取计算机信息系统数据罪。据了解，在今年9月初出台的最新司法解释中，对此类犯罪的“情节严重”“情节特别严重”作出了明确区分，本案也成为新司法解释出台后的国内第一案。

“新解释直接影响对他们的量刑。”承办法官说。昨天的庭审持续了大半天，法官宣布合议庭审议后，择日宣判。

□通讯员 关研 快报记者 张瑜

案件始末

他写的木马程序杀不掉

今年31岁的罗华是数学系出身，但计算机水平很高。大学毕业后，他进入北京一家科技公司做程序员，多次参加有关部门的重大工程，在国内外黑客界被公认为高手。

2008年底，罗华在QQ上结识了东北人苏强。苏强是一家网站的站长，那段时间他的网站总被人攻击，所以想请高手罗华帮忙，进行安全维护。作为报酬，苏强每月会给罗华的银行卡内打入一两千元。

身为顶级黑客，小小的网络攻击根本难不倒罗华，他很快帮苏强维护好了网站。2009年八九月份，苏强在和罗华网上聊天时，提起了很赚钱的盗号木马程序，并通过QQ发给罗华一个木马程序让他破解。罗华不仅破解了程序，还重新编写了一个新的木马程序。一旦玩家中了这种病毒，账号和密码会自动发到一个被称作“箱子”的地址里。

此外，罗华还为木马程序进行了“免杀升级”，这样一来，普通的杀毒软件就算及时更新升级，也没法查杀出这个木马。苏强很是满意，付给罗华5000元。随后，罗华还会定期对木马程序进行维护，苏强也会每月支付他200元到500元不等的费用。

应苏强的要求，罗华后来又做过“魔兽世界”“冒险岛”“永恒之塔”等游戏的木马程序，免杀升级让这些程序逃过了杀毒软件的眼睛。同时，罗华还给木马加密，防止别人偷他的程序。到去年下半年案发前，罗华从苏强手里拿到20余万元报酬。

中间人转给广西下家

苏强不会白给罗华报酬，他本人也获利7万元。事实上，苏强的角色是批发商，那些木马程序都被他卖给了远在广西的下家胡文林。

胡文林生于1984年，只有小学文化，平时爱玩网络游戏，因自己账号被盗过，便产生了再去盗别人账号的想法。去年11月左右，他遇到了苏强。

胡文林把盗窃别人的账号和密码叫做“洗信”，他先通过流量商在网上挂木马，玩家中毒之后，密码、账号等会被发到一个被称为“箱子”的固定地址里。胡文林还让苏强负责维护，每月费用在几千元到上万元不等，并找来了杨彬等5人帮忙，成立了“洗信工作室”。

胡文林和杨彬等人是老乡关系，平时，胡文林自己会联系流量商，搞到装备后拿出去卖钱，有时候也会让杨彬帮忙。其他4个人主要负责从“箱子”里拿账号和密码，胡文林会按月给大家发工资。从去年11月到案发前，胡文林获利五六万元，杨彬等人也都拿到上万元报酬。

由于杨彬做事比较多，有时候胡文林还额外多给一些，不过杨彬也不是个省油的灯，在“洗信工作室”期间，他还暗中将盗来的1万多组游戏账号和密码，卖给了一个叫丁晓猛的人，丁晓猛也通过卖游戏装备和游戏币等，获利数千元。

玩家报警让他们全部落网

2009年，曾有媒体报道，中国的木马产业链1年的收入达到了上百亿元。

去年11月中旬的一天，南京下关的一名游戏玩家上网时，突然发现他在“新奇迹世界”中的装备被人偷了。这位玩家十分恼火，因为这套游戏装备是他花了大力气才弄到手的，市值可能在2000元左右。

这名玩家事后了解到，装备被盗的原因，是有人用木马程序让电脑中毒，然后盗取了他的游戏账号和密码，于是赶紧报警。在此期间，还有多位游戏玩家也报了案，大家都反映自己的游戏装备、游戏币被盗，这引起了南京警方的注意。

随着立案和侦查，案情逐步清晰了起来。警方发现，这是一个完整的犯罪链，并掌握了木马程序的编程和维护者、被邀请写木马程序的上家、购买木马程序直接用于盗号的下家的情况。

去年12月开始，警方决定开始收网，到今年初，9名犯罪分子陆续归案。

值得一提的是，这些人落网时，警方从杨彬的电脑中发现，还有8900多组游戏账号、密码被存在其中，这都是他们还未来得及去卖的。

制图 李荣荣

现场直击

是否适用最新司解成为法庭辩论焦点

罗华昨受审 快报记者 张瑜 摄

> “大学毕业后，我就开始从事网络安全研发工作，并多次参加有关部门重要工程，我非常喜欢这份工作……法律意识淡薄，导致我误入歧途。
> ——罗华

昨天，这起危害计算机信息系统安全的刑事案件在下关法院开庭，苏强、罗华、胡文林、杨彬、丁晓猛等9名被告人出庭受审。这9人中，年龄最大的苏强33岁，其次是罗华，而胡文林等广西柳州的这7名被告都是出生于1984年。旁听席上，坐着被告家属以及法院邀请的特邀咨审员。

他自称法律意识淡薄

苏强、罗华被指控的罪名，是涉嫌提供侵入计算机信息系统程序罪，其余7人则被指涉嫌非法获取计算机信息系统数据罪。被告人都自愿认罪，法庭采取了普通程序简化审理。由于家属就在旁听席上，庭审中部分被告人频频回头。旁听席上一位老太太听得特别认真，她自称是其中一位的亲人，看着被告一个个走进法庭时，她悄声问身边的人，被告是否戴了脚镣。

罗华是9名被告人中唯一戴黑框眼镜的，看上去比较斯文。他安静坐在被告席上，回答法庭提问时，说话声音不大，很少举手发问。在今年1月被抓后，罗华很快积极退赃24万元，这也成为他后来在量刑中被提到的酌定从轻处罚情节。

此外，公诉人也指出，罗华在被关押期间曾为公安机关破获一起重要案件，所以算是重大立功表现。在最后陈述中，罗华情绪稍显激动。“大学毕业后，我就开始从事网络安全研发工作，并多次参加有关部门重要工程，我非常喜欢这份工作……”罗华说，因为法律意识淡薄，导致他误入歧途。

庭审中，苏强、胡文林等人尽管对部分内容提出异议，但都没有否认其犯罪事实。苏强也表示，他在案发后曾退赃8万余元，法庭要求公诉人庭后核实。

公诉人：情节特别严重

在阐述量刑意见时，公诉人指出，苏强、罗华向他人提供侵入计算机信息系统程序，情节特别严重，建议在3年以上7年以下有期徒刑量刑；胡文林、杨彬利用木马程序非法获取计算机信息系统数据，情节特别严重，也应在3到7年之间量刑；其他5名被告情节严重，系从犯，建议在3年以下量刑。公诉人还提醒法庭，注意被告人的法定从轻、减轻处罚等情节，比如丁晓猛当初是自首，所以应予以考虑。

庭审之前，媒体关注的一个关键点，是新的司法解释对这9名被告人量刑的影响。今年9月初的最新司法解释是否适用，也确实成为了昨天法庭辩论的焦点之一。罗华的辩护人就说：“按照最高法的解释，被告人的情节属于特别严重，但是请法庭重视一点，被告人的犯罪行为是在最高法新的解释出台之前，所以希望法庭对被告人的情节按照严重来判决。”不过公诉人却指出，在最新司法解释中，明确规定今年9月后后审理的案件适用此解释。

此外，针对辩护人提出杨彬应被认定从犯的说法，公诉人认为杨彬与胡文林属于共同犯罪，不宜区分主从犯。直到昨天下午两点，庭审结束。法官宣布闭庭，由合议庭审议择日后宣判。

法官解释

何为“严重”和“特别严重”

庭审结束后，记者采访了审理这起案件的下关法院刑庭副庭长胡斌兵。针对庭上控辩双方讨论的最新司法解释，胡斌兵作出了解答。

胡斌兵指出，2009年2月28日，《刑法修正案（七）》就增设了计算机犯罪的相关罪名，其中就包括本案中提供侵入计算机信息系统程序罪、非法获取计算机信息系统数据罪。今年9月最新司法解释出台前，法律没有对此类犯罪的“情节严重”“情节特别严重”进行区分、认定，没有规定具体的认定标准，这给办案部门带来了难度。

“最新的司法解释，有了明确区分。比如提供侵入计算机信息系统程序的，违法所得超过5000元的就达到情节严重入罪了，非法获取计算机信息系统数据的，获取认证信息500组以上的，也被视为情节严重入罪。情节特别严重是数量、数额达到标准的5倍以上，比如违法收入在2.5万元以上，获取信息2500组以上的。”胡斌兵介绍说，本案中的苏强、罗华违法所得7万、20万，都构成了情节特别严重。还有6位被告获取信息被认定是8900多组，也都算是情节特别严重。

（文中案件当事人系化名）