全国最大Q币犯罪产业链揭秘

轻松窃取千万用户信息，非法获利600余万元

□新华社“新华视点”记者 王晓磊

核心提示 这是一条全国最大的“Q币犯罪产业链”——一伙由青年人组成的犯罪团伙涉嫌对上千万台电脑用户植入木马，占中国互联网盗窃Q币犯罪产业链总规模的近80%，且形成了制作木马、研发辅助软件、挂马、盗号、洗信、贩卖Q币等犯罪全程流水线作业。

重庆挖出的网络犯罪大案，再次敲响信息安全警钟：如何斩断伸向网络信息的“黑手”？

全程流水作业的“Q币犯罪产业链”

Q币是腾讯公司开发的网络虚拟货币。Q币犯罪，是指一些不法分子趁机窃取电脑用户信息及其Q币，再转卖获利的违法犯罪行为。近日，重庆挖出了一条横跨全国的开发制作、策划组织、指挥种植“木马”，再通过“木马”植入盗窃QQ信息，将Q币进行网上销售的网络犯罪产业链。

今年2月，重庆市公安局网安总队接到多起群众报案，称QQ号码和Q币被非法窃取。警方调查发现失窃的Q币都被换成网络游戏“QQ仙侠传”中的元宝进行了转移，接收者是一个名为“小懒虫”的游戏ID。他仅一个月内便涉及交易QQ号码1471个，折合人民币近29万元。

经调查，“小懒虫”梁某是重庆合川人，与妻子明某在淘宝网开设了一间名为“懒虫猫小宝”网店。从2011年7月起，梁某夫妻通过在网店贩卖“QQ仙侠传”元宝，获利达86万余元人民币。警方循线追踪，挖出了梁某的主要联系人“亮亮”。

通过海量数据侦查比对，一个庞大的网络盗窃Q币犯罪链条浮出水面：

一是策划、组织、指挥工作，由网名为“亮亮”的犯罪嫌疑人吴某负责。他系网络犯罪圈内的“知名人物”，具备较强号召能力和丰富的“从业史”。

二是“洗信”和“挂马”，前者由犯罪嫌疑人尹某负责，即按照“亮亮”授意，对盗窃而来的用户QQ信息进行分类处理；后者系网名“香草”的犯罪嫌疑人翁某等五人以“楠天网络科技公司”作为掩护，通过种植木马病毒，控制客户主机的方式，大肆开展攻击，导致用户电脑感染；

三是开发盗号辅助软件，犯罪嫌疑人吴某等三人自行开发软件后协助“亮亮”传播木马，收取费用分成；

四是销售环节，如犯罪嫌疑人梁某及其妻子犯罪嫌疑人明某，从“亮亮”处以7.0折到7.3折的折扣买进Q币，以游戏元宝形式在网店以7.9折出售，赚取差价。犯罪嫌疑人和某等三人也在“亮亮”指使下，协助梁某夫妇进行销赃活动。

由于犯罪嫌疑人分散在全国各地，今年3月11日，专案组7个抓捕小组在重庆、海口、杭州、福州、泉州、保定、成都同步出击。当日23时45分，18名犯罪嫌疑人全部归案。在进一步侦查中，警方又将“神秘”的木马制作者——武汉某大学研究生二年级王某抓获。

经调查，该团伙自2011年3月以来，涉嫌对1000多万台电脑植入木马，盗取Q币进行贩卖，非法获利600余万元。同时他们还将被盗QQ号码广泛用于诈骗好友、靓号买卖、微博推广、垃圾短信等违法犯罪活动。

犯罪特征：智能化+隐蔽性，低成本+高收益

十几名犯罪嫌疑人，何以能在不长的时间内轻松窃取了上千万电脑用户的信息，作下震惊全国的大案？网络信息安全大案屡发原因何在？

重庆警察学院刑事侦查系教授菀军辉说，主要原因之一是当前网络信息犯罪的智能化、隐秘性强，且多为跨区域作案，侦查取证难。记者了解到，此案中犯罪嫌疑人制作和传播木马、挂马、洗信、贩卖Q币等均全程智能化操作；团伙成员遍布各地，之间以虚拟身份联系，资金往来也依托虚假银行账号，并通过各种技术手段隐匿个人真实信息，这些都为警方侦查、取证带来了前所未有的难度。

办案人员说，在进行抓捕时，警方是在前期缜密侦查后同步出击，才将嫌疑人一网打尽的。否则，团伙成员之间一旦察觉对方网络联系中断，即可能在第一时间销毁各类电子物证，令侦查工作前功尽弃。

犯罪成本低、收益高，反复作案几率大，也是网络信息犯罪屡禁难绝的原因之一。菀军辉说，犯罪嫌疑人只要掌握了一定的计算机操作技能，即可实施此类犯罪，且收益往往极高，如木马制作者王某前后获利近50万元。在取证时，由于受害的QQ用户遍布全国，盗窃数额难以固证，且过去取证不充分，司法处理较轻，涉案人员反复作案几率大，造成恶性循环。

以此案中的核心成员“亮亮”为例，他在2009年曾因非法入侵计算机信息系统案被打击处理，但仅获刑11个月便又“重出江湖”。低犯罪成本和高收益促使其再度铤而走险。

与此同时，犯罪嫌疑人利用了网民一些不健康的上网习惯进行传播，也是该类犯罪行为“传染性”很强的原因。以此案为例，木马开发者针对网民的猎奇心理，瞄准色情网站进行传播。网民一旦浏览特定的色情网页或下载特定软件，电脑即被感染。办案人员表示，此案中海量的受害用户，说明了当前不少网民仍亟待树立健康的网络价值观。

如何让青少年远离网络信息犯罪“黑手”？

在此案中，最让人触动的是嫌疑人的低龄化。记者了解到，该犯罪团伙是一群“青年军”，年纪最大的不过30岁、最小的仅21岁。例如其核心成员“亮亮”是一名“90后”，自未成年时就开始实施此类犯罪；制作木马的犯罪嫌疑人王某更是具备较强的软硬件制作能力，2010年因成绩优异保送研究生，在校期间还曾获全国电子设计大赛二等奖。临近毕业的他已获得多家著名网络公司青睐，而王某打算从事的居然是互联网账户安全保护工作。但由于他一念之差，在百度空间上炫耀木马技术，被“亮亮”相中，走上犯罪道路。

专家表示，鉴于网络信息犯罪多发、一些青少年误入歧途的严峻形势，必须由司法部门、网络运营商、广大网民形成合力，对网络信息犯罪实现“立体化”清剿，同时将打击和教育相结合，让青少年远离网络犯罪。

腾讯公司相关负责人表示，一方面将继续配合国家相关部门，对盗号、盗币等严重侵害QQ用户权益的行为进行打击，最大限度保障QQ用户权益。另一方面，还将重点从技术方面对盗号行为进行打击，保障平台的健康、安全。

“广大青少年网民还应加强防范意识，形成健康的上网习惯。”重庆一家大型综合性网站社区部负责人罗林说，许多木马均依托色情网站进行传播，网民切勿点击浏览，更不要下载来历不明的免费软件、插件。虚拟货币一旦被盗，应及时报案，积极提供破案线索。

办案人员认为，依法加大惩处力度，提高犯罪成本，也是有效打击网络信息犯罪的关键。记者了解到，此案中所有涉案电子物证已及时勘察和查封，由于侦查严密、取证充分，目前检察机关已经以涉嫌盗窃犯罪对吴某等11名主要犯罪嫌疑人批准逮捕。他们面临的将是法律的严惩。

（据新华社重庆5月14日电）