“钓鱼”邮件盗QQ号骗走86万元

警方破案后发现,嫌犯制售木马已盗号120余万个

先给你发邮件植入木马,盗取你的QQ信息;再远程监控你的QQ聊天,摸清你的关系网,伺机发出诈骗信息。近日,莒南县警方破获一起特大网络诈骗案,制售电脑木马者竟将木马卖给全国1400余人,盗取的QQ号码达120余万个,其中仅莒南一家企业就因出纳QQ被盗而受骗86万元。

文/片 本报记者 高祥 本报通讯员 徐家伟 徐向田

涉嫌制售木马病毒的犯罪嫌疑人萧某被警方抓获。

QQ上直呼其名,“老总”让出纳汇款

今年8月17日上午11点多,莒南一企业财务部出纳邬莺莺上班时,公司总经理“赵鹏”突然通过QQ给她打招呼,并直呼其名。

“赵总”,邬莺莺急忙回应。“赵总”问:“咱们公司账上还有多少可用款?”“稍等,我给查一下。”邬莺莺告知后,“赵总”回复“马上打86万元来,有一笔款需要支付”,并发来一个农行账号。“赵总,付款用途写什么?”邬莺莺小心地问道。“备注,往来款。”对方回答。

丝毫没发觉异样的邬莺莺赶紧按照财务流程,将86万元汇了过去。

当日下午2点半,邬莺莺把此事向财务总监刘燕作了汇报。一听说“赵总”是通过QQ发送汇钱指令的,刘燕警惕地问道:“你与赵总通电话了吗?”邬莺莺回说:“打了赵总的手机,可没有打通。”

刘燕急忙给总经理赵鹏打电话核实,的确无法打通。刘燕又给他的妻子打电话,在得知他从来不玩QQ,更没有使用昵称为“赵鹏”的QQ号后,刘燕意识到被骗了。

怀着最后一点希望,刘燕赶紧致电银行,查询那个可疑的农行账号。很快,最不愿看到的结果出现了:86万元已在3个小时内被全部取走。

千里追踪“木马”,捉到幕后“大鱼”

受骗企业是莒南一家以生产生物发酵产品为主的大型公司,拥有员工6000多人。公司被骗后,在当地造成较大影响。莒南警方迅速成立专案组,开展调查。

技术民警对邬莺莺及其他员工的电脑进行了勘验取证,提取了诈骗嫌疑人发送的含有木马病毒的“钓鱼”邮件,经过分析,确定犯罪嫌疑人的活动地点为广西宾阳县。

8月19日,专案组飞赴1700余公里外的广西南宁。在当地警方配合下,专案组调取了犯罪嫌疑人取款的广西马山县、都安县、宾阳县等各个ATM机的监控视频。但是,由于涉案人都进行了精心伪装,监控并未拍下其面部特征。

专案组另辟蹊径,倒查银行流水,进行了海量的数据分析;同时,又对“钓鱼”邮件追踪溯源,最终锁定了犯罪嫌疑人萧某。

经查,25岁的宾阳人萧某,正是此案中木马病毒的制作者。

11月4日,萧某及同伙陆某被抓获,同时被没收的还有电脑等作案工具、涉案赃款30余万元及奥迪轿车一辆。民警在萧某的木马平台上查验得知,他已经向全国1400多人出售过木马病毒,盗取的QQ号码达120余万个。

嫌犯“苦心经营”月余,觅得作案良机

据办案民警介绍,从萧某处购买木马病毒并对莒南县这家公司进行诈骗的团伙,因同时涉嫌诈骗天津一家企业,大部分成员已被天津警方抓获。受害公司被骗的86万元款项已有部分被追回。

据调查,早在案发前一个月,该公司财务部职员的QQ邮箱便收到了犯罪嫌疑人发送的“钓鱼”邮件。7月16日至案发前,嫌疑人还伪装成邬莺莺的QQ邮箱,以“人事调动通知书”“事业单位工资调整方案”等诱惑性内容,给该公司6名财务部职员发送含有木马附件的邮件,寻找作案目标。多人不疑有诈,打开邮件附件后被植入了木马病毒。

据犯罪嫌疑人交代,嫌人木马病毒后,他们会随时跟踪受害人的邮件往来和QQ聊天信息,并据此分析公司人员的角色分工甚至性格特征。

案发前,犯罪嫌疑人远程监控受害人的QQ发现,该公司总经理赵鹏会于8月17日坐飞机。嫌疑人精心选择赵鹏在飞行途中无法打手机的这一绝佳时机,模仿赵鹏的语气对邬莺莺发送汇款指令,从而成功地实施了诈骗。(文中受害企业当事人均为化名)