浅析QQ盗号木马的工作机制

姓名：袁昊男 学号：2018091618008

QQ被盗号情况时常发生在生活中。“盗号”指不法分子通过非正常手段获取用户的QQ账号以及密码。在过去年代，QQ未启用风险识别模型与双重认证机制时，不法分子可以用获取到的账号及密码轻松登录被害人账号，进行诈骗等违法行为。但如今QQ的风险识别策略非常先进，即使不法分子获取到了用户的QQ账号与密码，也无法顺利登陆。如QQ在检测到某账号的登陆IP与设备并不是用户的常用IP与设备时会自动开启双重认证机制，要求用户使用短信验证码或人脸识别等二次认证方式登录账户。且用户在发现账号被盗号后，可立即冻结账户并强制对方下线。种种风险控制策略在很大程度上避免了损害用户权益的行为发生。如今的QQ盗号木马所发挥的作用虽远远不及从前，但还是很有必要对其工作机制有大致了解。

黑客盗取QQ账户主要有两大类方式。一种是在本地环境中采用各种手段获取他人电脑使用权后，利用某些破解工具对临时存储在本地的账号密码加密文件进行破解。另一种是在互联网环境中通过各种盗号木马或钓鱼网站进行窃取。本文主要概述在互联网环境下远程盗取QQ账号密码的原理。

步骤一：黑客首先在互联网中申请一个ASP空间或一个电子邮箱。

步骤二：将申请好的ASP空间地址或电子邮箱地址填入控制端软件的配置文件，生成相应的接收程序文件，通常为ASP类型。

步骤三：利用FTP工具将QQ木马控制端软件生成的接收程序文件上传至ASP空间。

步骤四：控制端软件可自动生成QQ木马，其中包含了接收地址信息。生成木马的扩展名为“exe”。

步骤五：将生成的木马进行一系列的伪装、捆绑或免杀处理。黑客会将木马程序图标伪装成腾讯QQ企鹅图标、并命名为“QQ绿色纯净版”、“QQ新功能版”等，有时会将伪装好的木马程序与正常应用程序进行捆绑。一些高级黑客会对生成的木马进行免杀处理。所谓“免杀”是指利用“定位病毒特征码技术”和“反汇编技术”对木马进行二次处理，使其避免被杀毒软件查杀。

步骤六：黑客通过Internet将这些经过层层伪装的QQ盗号木马以各种形式传播至他人计算机。通常的传播方式有以下几种：

1. 以好友身份将捆绑有木马的文件通过QQ发送，请求对方接收。
2. 向对方发送带有木马的E-mail附件，诱骗对方接收。
3. 搭建挂有木马的网站，诱骗好友访问；或无目标性地将网址发布到各种论坛、贴吧中供网友访问。用户一旦访问此类网站，计算机会立即被感染。
4. 将木马捆绑至各种游戏外挂程序中供游戏爱好者下载使用。

步骤七：用户一旦接收到这些捆绑木马的文件并双击运行，会立即激活木马。对于QQ盗号木马而言，通常会出现两种情况：

1. 弹出酷似QQ登录的伪界面，用户将QQ账号和密码输入伪登录界面后，立即会弹出各种奇怪的QQ软件出错提示，随后自动关闭此界面。与此同时，木马已将账号和密码从内存中截取或用键盘记录器记录。这些莫名其妙的错误提示只是掩人耳目的手段，给用户一种软件出错的错觉。
2. 某些盗号木马双击运行后首先强制关闭正在运行的正常QQ程序，用户发现QQ自动下线后，再次运行正常的QQ软件输入账号和密码，此时输入的信息已被驻留在内存中的木马所截取或用键盘记录器记录。

步骤八：由ASP空间中的接收程序调用受害者计算机中的木马将截取后的账号、密码信息自动上传至ASP空间。如果黑客使用的是电子邮箱，此时受害者计算机中的木马会自动向指定邮箱发送包含账号、密码信息的邮件。

步骤九：利用FTP工具登录ASP空间，将包含有QQ账号、密码信息的文件下载至黑客本地电脑，或登录邮箱获取账号信息邮件。

至此，黑客完成了一次完整的盗号过程。

如今大部分的QQ盗号并不是通过本地盗号木马完成的，往往是通过钓鱼网站仿冒腾讯公司旗下各种网页，要求用户在网页中输入QQ账号及密码，从而完成盗号。不管是本地木马盗号还是钓鱼网站盗号，普通用户都可以通过以下几种方式有效避免盗号行为发生：

1. 使用官网正版软件，不执行来源不明的exe可执行文件。
2. QQ登录界面中输入账号密码时不应选中“记住密码”和“自动登录”复选框。
3. 不随意在网页中输入账号及密码，确有需要必须输入时，先查看网页域名是否以“qq.com”结尾，否则即可判断为钓鱼网站。
4. 开启QQ账户的双重验证功能。

互联网是一把双刃剑，以腾讯QQ为代表的网络即时通讯工具也是如此。只有真正了解了木马病毒的特性及实施原理才能使广大网络用户更好地进行安全防御。