教你几招识破“浮云”网购大盗木马

启明星辰安全研究团队

近来，网购大盗木马“浮云”再次肆虐网络，黑客通常通过旺旺，QQ 等聊天软件将病毒传给用户，并用社会工程学的方式诱使用户打开。文件名往往为“实物图”，“宝贝介绍”等具有诱惑性的名字。下面结合该病毒的最新诈骗手段教大家几招快速识别类似网购木马的手段。

病毒主要诈骗过程分析：

1. 黑客通过旺旺，QQ 等聊天软件将病毒发给用户，并诱骗其打开。
2. 病毒往往由完整合法数字签名的 exe 文件以及相应的动态库，数据文件等等组成。具有合法数字签名的 exe 文件往往会有 DLL 加载漏洞（未验证所加载的动态库是否合法）。这样病毒便可以利用数字签名绕过杀毒软件主动防御。相应的动态库（通常为病毒）被加载后，会解密另外的一个数据文件（网购大盗的主要功能），解密后将该数据文件完整的注入到一个系统进程中。
3. 病毒运行后，通常会弹出一个欺骗用户的对话框，提示“**失败”，“**无效”等等。
4. 之后病毒会结束当前所有的浏览器进程，然后会不断遍历浏览器窗口。当用户访问网购网站并进行支付的时候，会篡改支付网页。同时将用户购买的钱数，银行等信息发给黑客服务器，黑客服务器在处理后会发送一些信息回来，此时木马会根据黑客服务器发送回来的信息在后台利用浏览器登录其他一些网站实施购买点卡，充话费等的消费过程（而在此过程中可能需要用户填写验证码等，这些过程无法通过后台自动化完成，于是木马会在适当的时候将验证码的填写返回给用户，让用户填写）后台下好订单之后，弹出相应的付款页面供用户付款（此时付款页面的收款人不是用户网购时的收款人，于是木马会将付款页面“收款方”部分覆盖为用户网购的收款人以欺骗用户）

下面以淘宝为例揭秘欺骗全过程：

1. 篡改付款页面，使得用户只能用网上银行付款，其他功能被隐藏或者提示“正在维护”。

中毒现象 1、这里正常情况下有快捷支付栏目，但被隐藏。

中毒现象 2、其他一些付款方式提示“正在维护”

对比正常情况下，我们可以选择除了网上银行的其他支付方式。比如快捷支付等。

2. 在用户选择了相应的网上银行后，病毒会篡改“登录到网上银行付款”按钮的相应脚本代码，劫持用户正常付款流程。此时病毒会在后台向黑客服务器发送用户付款钱数以及银行名称。黑客服务器会返回一些数据。病毒利用返回的数据在后台登陆其他一些网站（比如 10086,ztgame,chinapay 等）下订单。**而在后台下订单的过程中通常会要用户输入验证码。此时病毒会将验证码的输入过程返回给用户，让用户填写。因此当发现莫名其妙的要求输入验证码的时候就要提起高度注意了！**

中毒现象 3、莫名其妙的弹出验证码错误的提示框，并让用户输入验证码。正常情况下此处是没有验证码的！

3. 在用户输入验证码之后，会用一些假的遮罩层覆盖住当前网页以等待后台订单提交成功。此时，注意左下角的 IE 访问网页提示，会发现访问了其他网站。

中毒现象 4、假遮罩层显示“正在检测您的帐户安全状态，请稍候”，IE 左下角显示正在访问的网页域名为 pay.ztgame.com 等并非当前交易中应该出现的网站

正常情况下，这里的遮罩层应该是这样。上面的“正在检测您的帐户安全状态，请稍候”明显是假的！

4. 最后付款的时候，由于收款人不是支付宝公司，因此病毒会将真正的收款人，钱数等信息隐藏，并用正常的将其盖住。此时可能会出现开始的瞬间是真的付款信息，而之后几秒内被病毒遮盖的现象。因此请特别注意这时的网页内容变化。

打开付款页面的瞬间，可能会显示成这样。此单真正的付款金额为 2000 元，且是给黑客充了游戏点卡。

稍候，病毒会将其遮盖成这样，显示正常的收款人以欺骗用户。