**网购退款多骗局**

经过几年的市场培育，年中各大电商平台促销盛典已经成为“剁手党”的血拼大事件。随着“6·18”的临近，剁手党们已经开始摩拳擦掌，网购狂欢即将上演。不过，此前支付宝、携程等接连故障宕机，网购安全也引起了人们的重点关注。对此，360安全专家提出了三大注意事项：谨防钓鱼网站、退款诈骗和手机木马。

**骗局一、钓鱼支付**

“6·18大促！限时抢购！买一送一！”剁手党们作为网购老手，常常利用搜索引擎货比三家，看到这样诱人的标语，往往克制不住点击的冲动，一不小心，就栽进了不法分子精心搭建的钓鱼网站。



360安全中心反钓鱼系统数据显示：每天检测到的虚假购物类钓鱼网站多达2000多个，平均每天拦截此类网站的访问量达150多万人次。利用这些钓鱼网站，只需如下四步，骗子就能成功敛财：

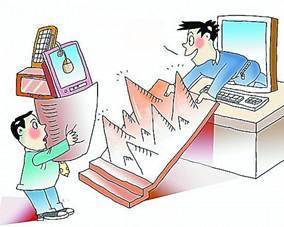
第一步租用一个服务器，注册域名；第二步根据需要复制、加工某购物网站，以假乱真；第三部通过竞价排名在搜索引擎拿到好的广告位置，以此招揽被钓鱼者；第四步就是通过钓鱼网站虚假交易等形式实施诈骗。



360安全专家表示，不要轻信远低于市价的商品信息，不要随意访问陌生网站或打开别人发来的网址链接，可以使用360安全卫士和360手机卫士等备钓鱼网站拦截功能的安全软件，可以有效帮助鉴别和拦截PC和手机上的钓鱼网站。

**骗局二、退款诈骗**

刚刚网购完，就接到了归属地显示为异地的电话，自称淘宝等电商网站店主或客服，提供了你的正确姓名甚至订单号，然后声称因系统问题，账单出现了异常，比如你的钱“卡”在支付宝了，系统升级导致订单被冻结等等，需要重新支付或退款。小心！如果碰到这种情况，那么很可能是遇到网购退款诈骗。



360安全专家介绍，网购退款诈骗，是当下最流行的一种网络诈骗手段之一。这种诈骗的主要形式是骗子冒充卖家，通过电话、聊天工具等方式（以电话为主）与刚刚完成网购的用户进行联系，谎称其刚刚购买的商品出现交易异常，并在“指导”用户进行交易异常处理时，诱骗用户进入钓鱼网站并进行支付操作，最终骗取用户钱财。



专家提醒，所谓的“卡单”、“掉单”、“交易异常”、“解冻订单”、“异常订单处理”等词汇全部都是诈骗专用术语，淘宝、京东等正规电商的网络交易平台上不会出现这些词汇。目前，淘宝网等电商网站的官方电话已经通过360手机卫士电话号码认证平台验证，用户在接到类似电话时，可以用360手机卫士辨别真伪，避免上当受骗。

**骗局三、手机木马**

随着手机支付越来越普及，不少剁手党早已将手机网购和支付作为首选。殊不知，手机木马也瞄准了剁手党们的手机。随着各大电商年中大促的开始，各种支付类手机木马更是如雨后春笋般层出不穷。



近日，360手机安全中心就拦截到了一款名为“购物狂终结者”的手机木马，该木马利用手机用户的网络购物需求，伪装成购物软件诱导用户下载，一旦用户安装运行，木马就会在后台私自发送扣费短信、上传中招用户手机信息等，造成手机用户隐私泄露以及话费损失。

还有一些手机木马甚至会长久的潜伏在用户手机里，伺机盗取银行卡账户、密码，以及银行发送的短信和验证码，盗刷银行卡里的钱财。



360手机安全专家建议，手机用户应尽量选择360手机助手等正规手机应用平台下载应用，不要点击不明来源的链接、扫描来历不明的二维码下载应用。在“6·18”大促期间购物时，更要给手机安装360手机卫士等手机安全软件，实时保护手机安全。

**年中网购电商大促销 小心手机木马狂偷话费**

火热的6月，各大电商平台纷纷开始了“年中大促”的活动，手机木马也瞄准了各位“购物狂”的手机。近日，360手机安全中心拦截到名为“购物狂终结者”的手机木马，恶意篡改购物相关应用诱导用户下载，一旦用户安装运行，木马就会在后台私自发送扣费短信、上传中招用户手机信息等，造成手机用户隐私泄露、话费损失。目前360手机卫士已对该木马实现首家查杀。



除了年底的双十一、双十二，电商平台纷纷打出“年中大促”的促销口号，喜欢买买买的人当然不会错过这个机会，各类购物APP纷纷涌现，手机木马“购物狂终结者”也趁机盯上此类应用。

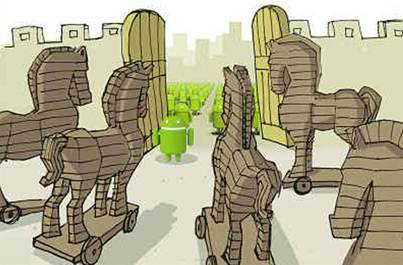
“购物狂终结者”恶意篡改九块九包邮等购物应用，诱导手机用户下载安装，点击激活后就会私自发送扣费短信，并屏蔽回馈短信，使中招用户无法察觉手机话费被恶意消耗；同时遍历手机通讯录向联系人群发短信，并将中招用户手机信息上传，造成中招用户隐私泄露。



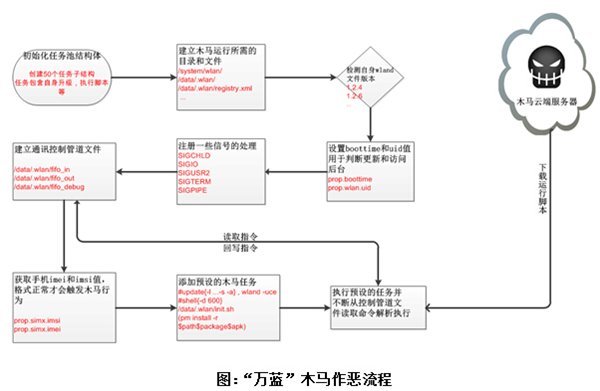
该木马利用手机用户的网络购物需求，伪装成购物软件诱导用户下载，给手机用户造成话费损失及隐私泄露。360手机安全专家建议：手机用户应尽量选择360手机助手等正规手机应用平台下载应用，不要点击不明来源的链接、扫描来历不明的二维码下载应用，同时给手机安装360手机卫士等手机安全软件，保护手机安全。

**安卓系统再曝ROM级木马“万蓝”**

今年五月中旬，360手机安全中心收到用户反馈称自己的手机经常自动安装新的游戏应用，经360手机安全中心分析排查发现，该用户中招的是一个名为“万蓝”的ROM级别手机木马，该木马影响用户达10万以上。该木马主要通过联网下载shell脚本文件进行静默安装推广应用，并可以实现自身升级。360手机安全中心发布技术博客，对“万蓝”木马进行详细分析。



360技术博客介绍，“万蓝”木马主要通过植入ROM，通过刷机网站进行传播。到目前为止，恶意样本主要是植入为夏新、联想、小采等手机开发的三方ROM进行传播，用户手机刷入被感染的ROM后，木马便疯狂地开始推广传播各种应用，总数高达近百种。



“万蓝”木马会联网下载shell脚本文件，把要执行的恶意行为写在脚本里，木马的wlan进程大部分功能在于执行这些脚本，这样就大大方便了病毒作者进行更新，也方便作者控制中招手机去执行更多恶意行为，潜在风险巨大。



技术博客分析指出，“万蓝”木马启动时会尝试给自身在系统目录中建立一些符号链接，当系统中有其它程序执行这些命令时，木马就会被启动。之后，通过初始化任务池、建立自身运行时所需的目录和文件进行手机木马初始化，为之后执行恶意行为做准备。值得注意的是，该木马启动后会初始化一个结构体，里面包含了50个可执行命令任务池的子结构。

360手机安全专家分析指出，“万蓝”木马是通过Linux管道来进行通信的，管道是Linux的一种通信方式，相当于一根管子，一个人在管子左边，一个人在管子右边，左边的人不停的往管子里放东西(写数据)，右边的人就不停的从管子拿东西(读数据)，右边的人拿到数据后就能够处理这些数据了，“万蓝”木马作者将要执行的命令、脚本写到管道里，之后wlan进程就可以执行这些命令。



木马从服务器上获取要运行的命令(shell脚本)，再调用诸如input、am、pm等系统命令，木马就可以实现启动应用、静默安装应用、卸载应用、结束应用、删除应用数据、结束后台进程、发布intent广播等40多种恶意行为。

此外，该木马还会通过两种策略实现自更新，一种是检测自身主体wland文件的版本来判断是否需要更新，一种是根据距离上次检测更新的时间来判断是否需要更新。该木马自升级以后还可以实现私发短信、屏蔽短信、拨打电话等恶意行为。



通过遗留在木马早期版本中的信息，360手机安全中心发现了木马作者以及公司的相关信息，通过木马链接的服务器地址判断，该服务器属于上海某科技公司，而木马作者也可能就职于该公司。

目前，360系统急救箱已经支持对该类恶意软件进行查杀，如遇到病毒反复查杀、手机自动安装软件等普通手机杀毒软件不能解决的异常现象，建议使用360系统急救箱进行查杀。同时建议手机用户从正规渠道购买手机，安装360手机卫士保护手机安全。