2016 中国电脑恶意程序伪装与欺骗性研究报告

360互联网安全中心

2017 年 1 月 3 日

360互联网安全中心

摘　　要

- 2016 年 360 互联网安全中心共监测到用户手动放行恶意程序 500 余万次，涉及恶意程序样本 3 万余个，平均每个此类恶意程序样本可以成功攻击 160 余台普通个人电脑。
- 通过对 3 万余个被用户手动放行的恶意程序样本的抽样分析统计显示，恶意程序最喜欢伪装的形式是游戏外挂为 31.7%。其次，贪便宜软件为 19.9%，色情播放器为 11.9%。
- 抽样统计显示，恶意推广是欺骗性恶意程序攻击的首要目的，46.4%的欺骗性恶意程序会在用户电脑上进行恶意推广，其次，远程控制为 18.2%，盗号为 13.2%，钓鱼充值为 9.7%，窃密和窃隐私类木马为 3.9%，敲诈者病毒为 2.8%。
- 恶意推广在伪装成各种形式的恶意程序中占比都比较高，特别是在贪便宜软件中，占比高达 52.2%，其次，破解软件为 48.7%，色情播放器 45.5%。
- 2016 年截获的欺骗性恶意程序中，伪装成游戏外挂的恶意程序样本数量在全年稳居第一，第二季度达到最高峰。与此相反的是伪装成贪便宜软件的恶意程序数量占比，第二季度处于最低峰，在第四季度超过了总量的 20%。
- 在伪装成各类游戏外挂，或捆绑各类游戏外挂的恶意程序中，恶意传奇私服类占比最高，达到了 31.6%，其次，小游戏类外挂为 23.1%，CF 类外挂为 13.1%，DNF 类外挂为 7.9%，LOL 类外挂为 5.3%。
- 抽样统计分析显示：刷 XX（如刷钻、刷会员、刷 Q 币等）在恶意贪便宜软件中占比最高，达 33.1%，其次是网赚挂机类为 24.1%，各类名称中含有领话费、领流量、领会员等字样的贪便宜软件恶意样本，占比约为 23.8%。
- 统计显示，37.9%的恶意色情播放器是通过用户浏览网页时突然弹窗的网站上下载的。其次，通过云盘、网盘等网络存储空间上下载，占比为 33.4%，通过捆绑其他软件传播为 11.2%，通过社交软件传播为 6.5%。
- 恶意破解软件最经常使用的名称是游戏破解补丁，占比为 33.7%，其次是网盘提速为 21.3%，系统激活为 12.9%，三者之和占到了此类恶意程序样本总量的 80%左右。
- 在伪装成常用程序与文件的恶意程序中，约 43.5%是伪装成了常用程序（系统组件、Flash 插件、应用程序安装包）。56.5%伪装成了各种文档或文件。其中，伪装成办公文档的约总量的占 34.9%，伪装成压缩包的约占 17.1%，伪装成图片的约占 4.5%。
- 统计显示，所有带后门的黑客工具中，扫描器排名第一，占比高达 33.9%，其次是 DDOS 工具为 16.8%；轰炸机为 13.7%，挖矿机为 15.5%，密码破译工具为 8.9%。

关键词：游戏外挂、贪便宜、色情播放器、破解软件、黑客工具、伪装、欺骗

360互联网安全中心

目　　录

研究背景

由于免费安全软件在中国的高度普及，恶意程序的编写、制作门槛越来越高，恶意程序的传播也变得越来越困难。自 2013 年以来，中国一直是全球个人电脑恶意程序感染率最低的国家。

但是，在全网监测中，我们也发现了一种奇怪的现象：有相当数量的用户，即便看到了安全软件的风险提示，也仍然会手动选择信任并运行恶意程序。统计显示，2016 年全年，360 互联网安全中心共监测到用户手动放行恶意程序 500 余万次，涉及恶意程序样本 3 万余个，平均每个此类恶意程序样本可以成功攻击 160 余台普通个人电脑。此外，还有相当数量的用户会选择临时关闭安全软件后再运行恶意程序。

用户为何会无视风险提示，手动放行，甚至强行运行恶意程序呢？2016 年 12 月，360 互联网安全中心的安全专家们对这一问题展开了深入的研究。研究发现，这些被用户手动放行的恶意程序在制作手法和攻击技术等方面并没有什么特别之处，也没有采用什么新型技术，安全软件对其进行识别和拦截通常来说并不太困难；但同时，这些恶意程序却普遍采用了社会工程学的伪装方法，从程序名，程序功能和界面设计等多方面进行精心的伪装，极具欺骗性、迷惑性。

本次报告专门针对这些被用户手动放行的，具有强烈欺骗性的恶意程序（简称：欺骗性恶意程序）进行深入的抽样分析研究，希望能够借此帮助更多的用户提高安全意识，有效防范此类恶意攻击。

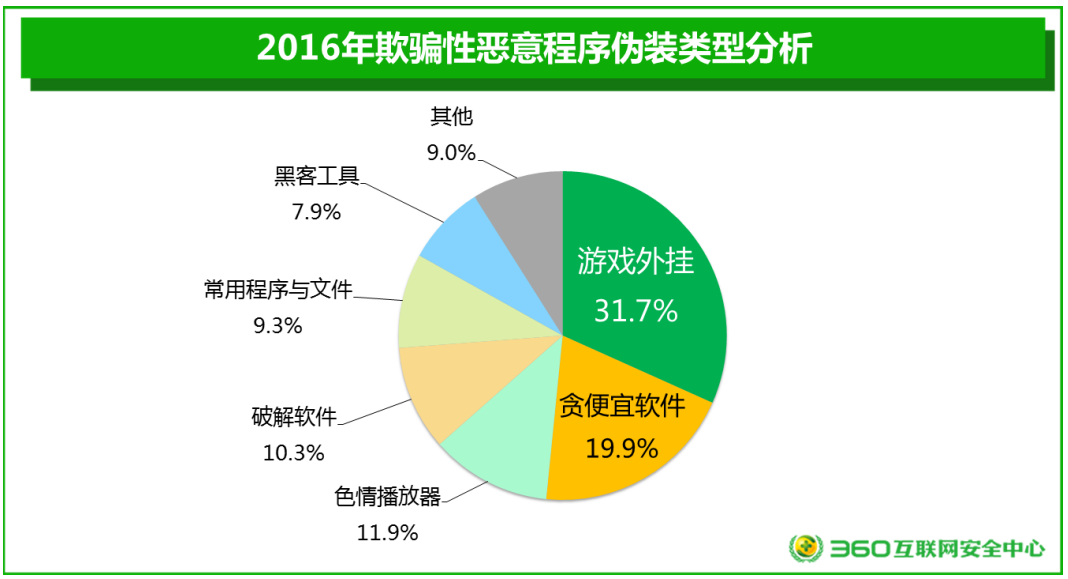
第一章　欺骗性恶意程序综述

一、　欺骗性恶意程序伪装类型

通过对 3 万余个被用户手动放行的恶意程序样本的抽样分析统计显示，这些带有强烈欺骗性的恶意程序最喜欢伪装的形式是游戏外挂，占比为 31.7%。由于很多用户会误以为安全软件会对游戏外挂软件进行无条件的风险提示，所以往往在看到恶意程序提示建议首先关闭安全软件再进行安装时，就会选择相信恶意程序，而无视安全软件的风险提示。但实际上，安全软件之所以会对某些外挂软件提示风险，主要是因为这些软件会携带恶意代码，一旦运行，就会进行流氓推广或释放捆绑的其他木马程序。

除了游戏外挂之外，恶意程序最爱伪装的形式排名第二位和第三位分别是贪便宜软件和色情播放器，二者分别占比为 19.9%和 11.9%。贪便宜软件是指那些自称具有刷金币、刷流量、领话费，以及外挂抢红包等功能，可以帮助用户赚点小钱的软件。而色情播放器则是指那些专门可以联网播放很多色情视频的播放软件。这两类软件很多都存在诱骗用户充值或进行流氓推广的行为。

此外，破解软件、常用程序与文件、黑客工具等也是这些欺骗性恶意程序比较喜欢的伪装形式。总体来看，除了伪装成常用程序与文件的形式外，恶意程序伪装的其他主要形式，或多或少都有一定的黑色或灰色性质，这些软件即便是不含有任何恶意代码的正常软件，其实际性质也基本上属于违法软件。所以说，相信和尝试使用非法软件，是受害用户被这些恶意程序欺骗的主要原因。



二、　欺骗性恶意程序攻击目的

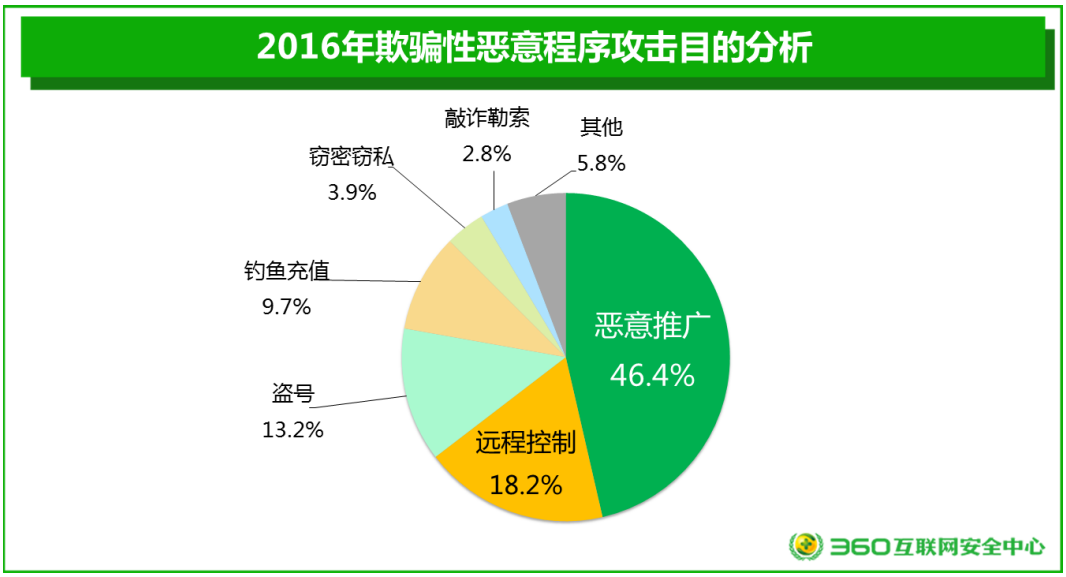
那么，这些经过精心伪装的欺骗性恶意程序一旦感染用户电脑后，会产生什么样的后果呢，这些程序攻击用户电脑的主要目的是什么呢？

抽样统计显示，流氓推广是欺骗性恶意程序攻击的首要目的，46.4%的欺骗性恶意程序会在用户电脑上进行流氓推广，它们通常会通过二次打包安装包等方式进行传播，不经用户

允许便私自静默安装各类推广软件，造成用户计算机变慢，并引发各类安全隐患，同时也造成用户心理上的不适感。还有一些进行恶意推广的恶意程序会释放一些带有参数的浏览器快捷方式，这些快捷方式指向浏览器并带有推广链接，有些甚至会直接锁定用户浏览器主页。事实上，流氓推广也是欺骗性恶意程序作者最主要的盈利手段。

欺骗性恶意程序攻击目的排名第二位和第三位的分别是远程控制占比为 18.2%，盗号占比为 13.2%，还有钓鱼充值占比为 9.7%，窃密和窃隐私类木马占比为 3.9%。

还有特别值得注意的是，有 2.8%的欺骗性恶意程序属于敲诈者病毒，它们的攻击方式非常特殊，是通过自动加密用户电脑文件的方式向用户索要解密赎金。国内敲诈者病毒勒索的赎金额度一般为 2-3 个比特币（现价约合人民币 1 万元-1.5 万元）。特别的，被敲诈者病毒加密的文件，绝大多数是不可能通过技术手段进行解密的。因此，敲诈者病毒在本报告分析的欺骗性恶意程序中虽然占比很少，但攻击危害极大，用户一旦手动放行此类恶意程序，便会立即产生非常明显的直接经济损失。



三、 伪装形式与攻击目的对比

下图给出了不同伪装形式的欺骗性恶意程序的攻击目的对比情况。

可以看出，流氓推广在伪装成各种形式的恶意程序中占比都比较高，特别是在贪便宜软件中，占比高达 52.2%，这就是最典型的贪小便宜吃大亏。

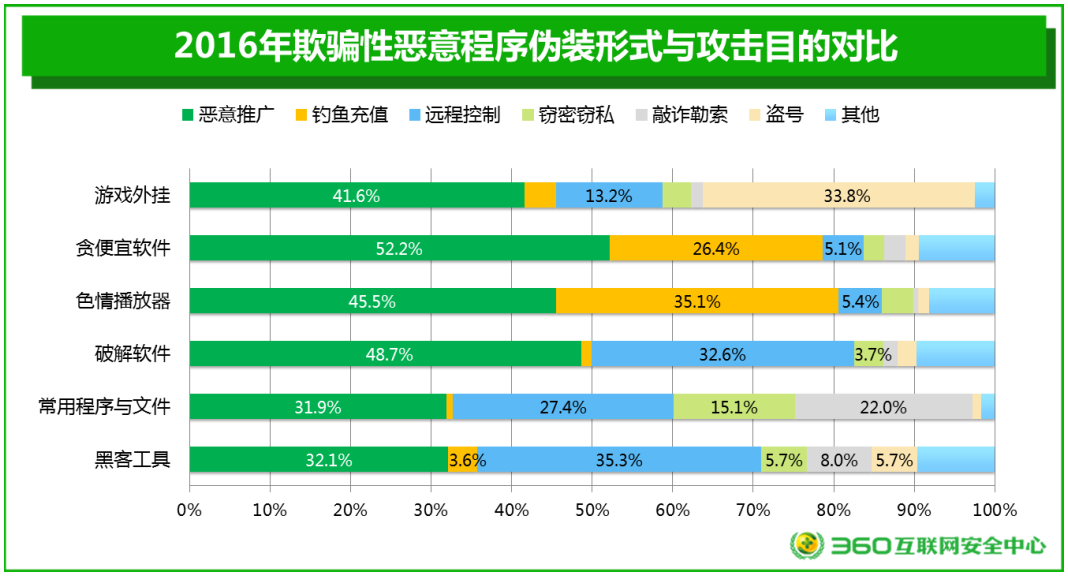
不过，不同的伪装形式和攻击目的之间也确实存在一些特殊的对应关系。

比如，在伪装成贪便宜软件和色情播放器的恶意程序中，钓鱼充值木马比较常见，占比分别达到了 26.4%和 35.1%。特别是伪装成色情播放器的恶意程序，常常会以各种暴露图片和色情视频吸引用户进行充值，但实际上用户无论充多少钱，都无法看到想看的视频，这种恶意程序是纯粹的欺诈软件。

再比如，在伪装成破解软件、常用程序与文件和黑客工具的恶意程序中，远控木马的占比都很高，都占到了 20%以上。这也警示了我们：在您企图走捷径（游戏外挂），或者是企

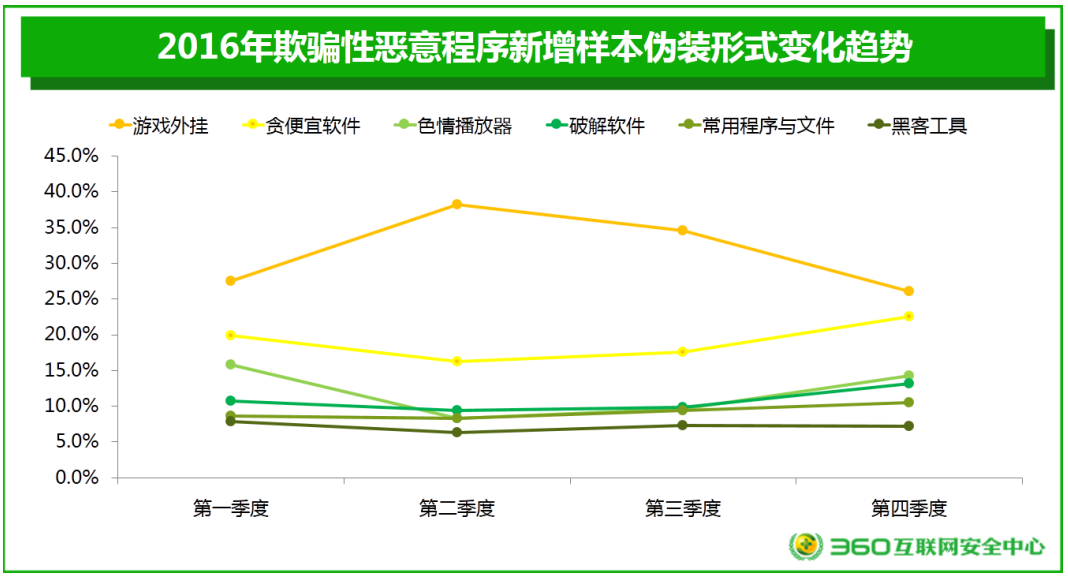
图用黑客技术操控他人（黑客工具）时，您也可能早已被别人盯上，成为被别人控制的对象。

再比如，在伪装成常用程序与文件的恶意程序中，敲诈者病毒占比最高，达 22.0%。这也再一次说明了一个安全意识的重要性：陌生人发来的陌生文件不要轻易打开。



四、 欺骗性恶意程序变化趋势

从新增样本的变化趋势来看，在 360 互联网安全中心 2016 年截获的所有欺骗性恶意程序中，伪装成游戏外挂的恶意程序样本数量占比全年稳居第一，第二季度达到最高峰，最后两个季度有所下降。与此相反的是伪装成贪便宜软件的恶意程序数量占比，第二季度处于最低峰，后两季度逐渐上升，在第四季度超过了总量的 20%，这也说明恶意程序作者比较偏向于选择此类软件作为载体进行传播。下图给出了不同伪装形式的恶意程序新增样本数量占比的全年变化情况。



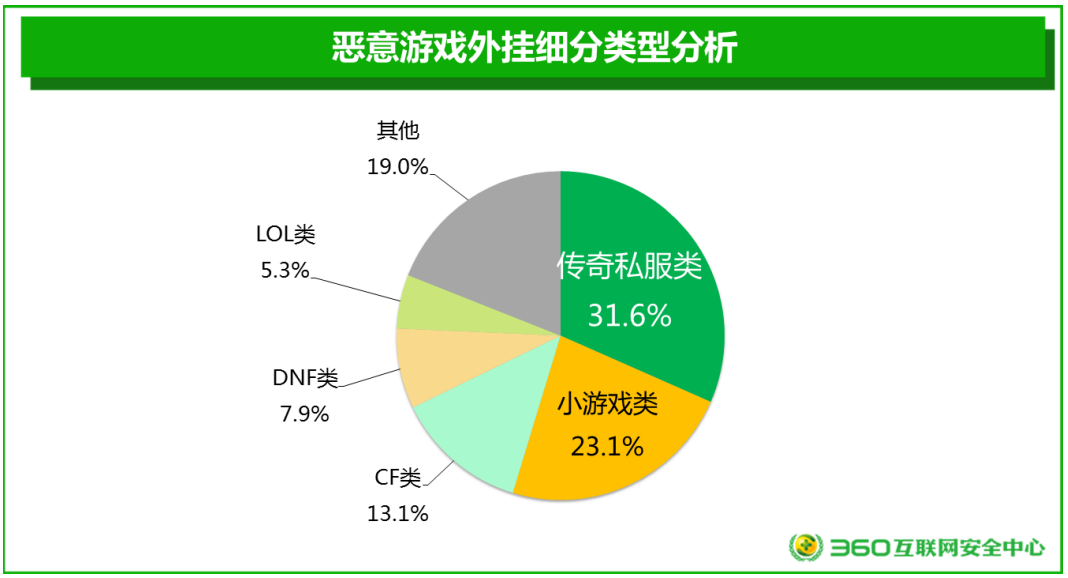
第二章　各类欺骗性恶意程序详解

一、　恶意游戏外挂类

近年来中国的互联网游戏迎来了突飞猛进的发展，可以满足不同年龄段用户需求，特别是 LOL、CF 还有各类游戏平台的小游戏等深受大众喜欢，玩家基数庞大，用户年龄段广。因此，恶意软件作者也瞄准了这块蛋糕，将外挂作为传播载体，捆绑木马或进行推广行为，从中谋取利益。

统计显示，在伪装成各类游戏外挂，或捆绑各类游戏外挂的恶意程序中，恶意传奇私服类占比最高，达到了 31.6%，原因是此类型的怀旧游戏玩家不少，多数玩家偏好私服，恶意程序作者也因此偏爱通过私服传播。该些恶意程序运行后会释放底层驱动程序，并从云端读取命令，劫持用户浏览器数据，锁定用户主页等。

此外，小游戏类外挂 23.1%，CF 类外挂 13.1%，DNF 类外挂 7.9%，LOL 类外挂 5.3%也都是欺骗性恶意程序最喜欢伪装的游戏外挂类型。



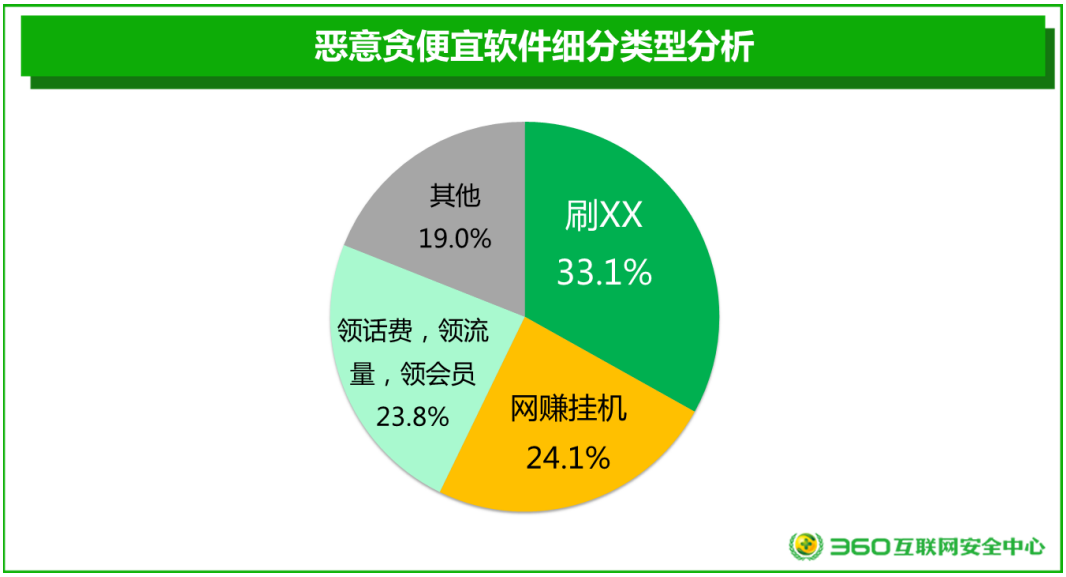
二、　恶意贪便宜软件

网络上的刷金币、刷流量、领话费、网赚挂机等软件层出不穷，其中大部分都是虚假的，恶意软件作者正是利用了“贪便宜”这种人性弱点，才让此类恶意软件日益猖獗。

通过对 360 互联网安全中心的抽样统计分析显示：刷 XX（如刷钻、刷会员、刷 Q 币等）在此类恶意程序中占比最高，达 33.1%，这归根于社交软件用户众多，并且部分用户喜欢追求某些特权，又不愿花钱，这直接导致了某些用户容易被此类恶意程序欺骗。

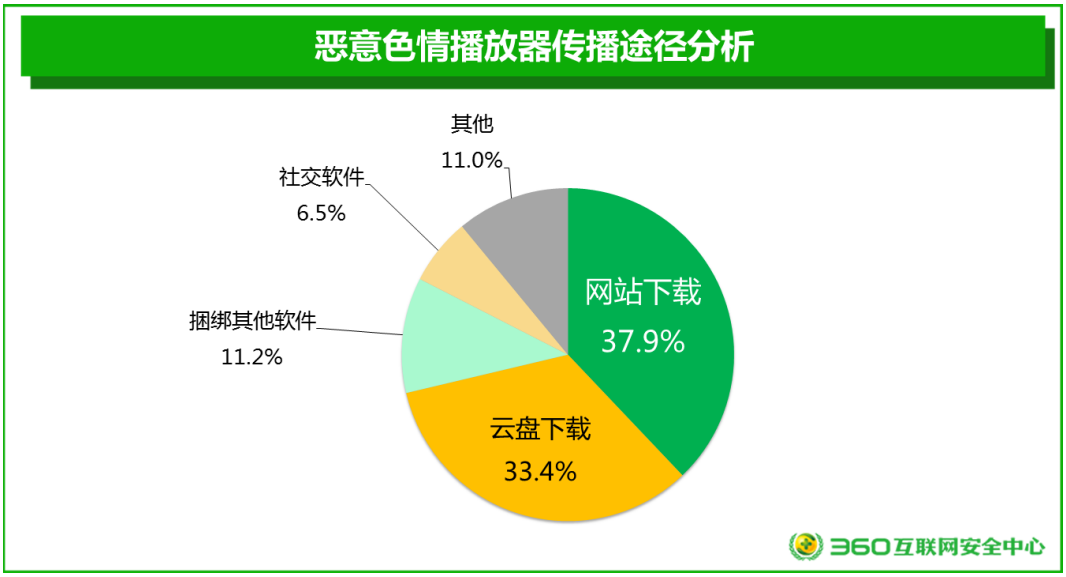
其次是网赚挂机类，达到了 24.1%，此类恶意程序通常宣称可以“自动点击广告”，“自动挖矿”赚钱，但实际上主要的行为是欺骗用户充值，伪装成各大银行以及支付宝等页面进行钓鱼盗号，流氓推广等行为。不过，对于普通用户来说，此类恶意程序在前期使用时往往无法及时发现其恶意行为，往往是当用户发现自己账户上的钱不断上涨，进行提现时才会发现其中的猫腻，发现钱取不出来。这也是此类程序占比较大的原因。还有各类名称中含有领

话费、领流量、领会员等字样的贪便宜软件恶意样本，占比约为 23.8%。



三、 恶意色情播放器

网上流传的绝大多数的色情播放器都是木马程序或捆绑了木马的播放器程序，其具体名称和外观伪装五花八门，这里不做详细分析了。但这类恶意程序的传播方式值得关注。因为其他绝大多数的欺骗性恶意程序之所以会被用户手动放行，一个重要的原因就是用户通常是主动去网站上查找相关功能软件（如游戏外挂、贪便宜软件、破解软件、黑客工具等），并主动下载和安装的木马程序。但恶意色情播放器的传播方式与此不同，很多用户是在不经意间看到了色情播放器的推广信息后，因被其内容强烈吸引而下载并安装的。



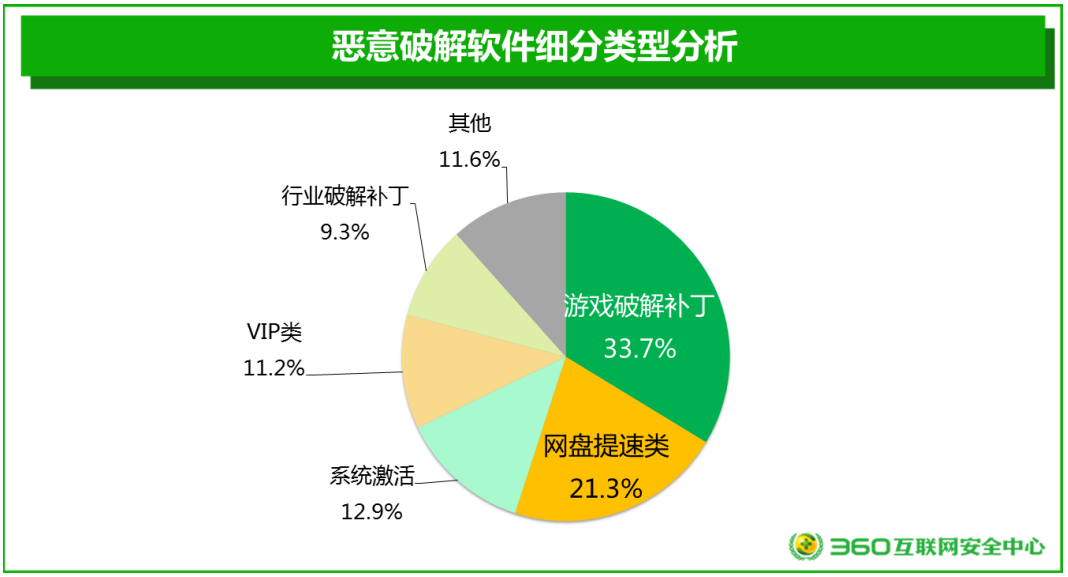
色情播放器通常是在用户浏览网页的时候突然弹出来的，也许是因为您不小心点了漂浮的广告，也有可能是您本来想下载软件，但点了“下载地址”后，莫名其妙就来到了一个奇怪的页面。一般来说，我们在遇到此类情况时，如果简单的关掉这些页面，通常不会有什么损失，但是如果按照提示安装了播放器，十有八九都会中招。统计显示，37.9%的恶意色情播放器是通过此种方式诱导用户在网站上下载的。

此外，通过论坛等渠道发布信息，诱导受害者到云盘、网盘等网络存储空间上下载，也是恶意色情播放器的常见传播方式，占比为 33.4%。在这种传播方式中，用户下载的安装包通常会被设置密码，目的是为了躲避查杀。再者就是捆绑其他软件传播，占比约为 11.2%，通过社交软件传播，占比 6.5%。

四、 恶意破解软件

尽管是在免费模式大行其道的当今互联网时代，仍然有很多软件、游戏是需要付费使用，或付费购买增值服务（如游戏装备等）的。但对于很多版权意识不强的用户来说，低价盗版软件，免费破解软件，或者是使用破解工具破解合法软件等，仍然具有一定的吸引力。所以，很多攻击者也就开始以免费的破解软件，破解补丁等名义，传播木马病毒。

恶意破解软件最经常使用的名称是破解补丁，云盘提速，以及系统激活这三类，三者之和占到了此类恶意程序样本总量的接近 80%。恶意破解软件通常会给用户静默安装推广软件，甚至植入后门木马进行远控。用户运行此类程序后，往往分不清楚这些软件的行为是破解行为还是恶意行为，又急迫的想要激活程序，因此在杀毒软件查杀时就会选择主动放行，忽略了其恶意行为。下图给出了恶意破解软件的细分类型分析。



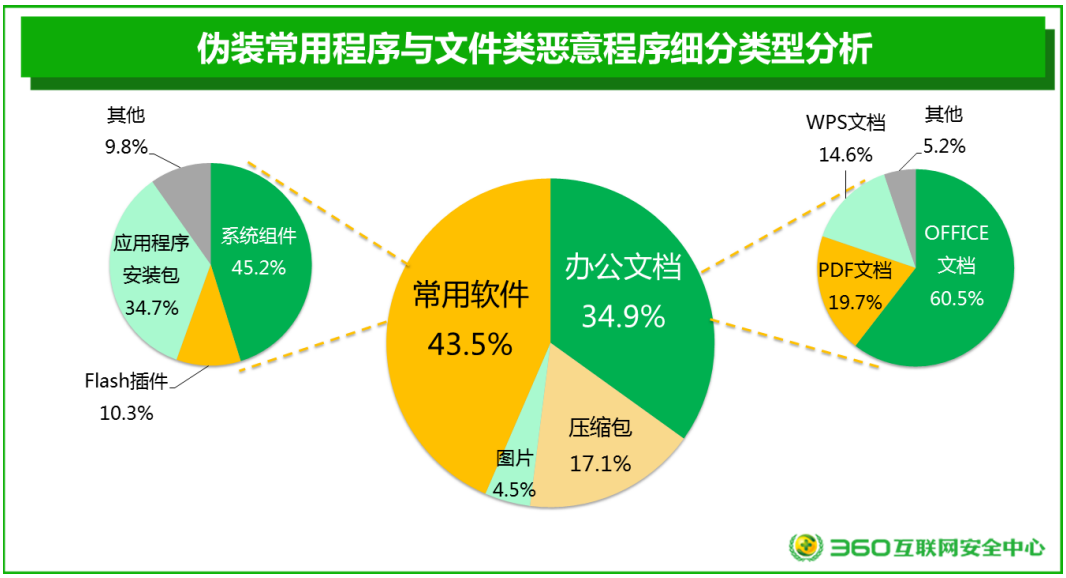
五、 伪装常用程序与文件

在本报告分析的所有欺骗性恶意程序中，伪装成常用程序或文件的恶意程序比较特殊，因为这类恶意程序并不是伪装成灰色或违法软件的形式来诱骗用户下载安装，而是尽可能的把自己伪装成一个看上去是“正常的”、“好的”，或者是用户“需要的”程序或文件，以此迷惑用户。

统计显示，在伪装成常用程序与文件的恶意程序中，约 43.5%是伪装成了常用程序，其中，比较常见的伪装形式包括系统组件（如 svchost.exe、rundll32.exe 等）、Flash 插件和其他一些应用程序安装包等。

另有 56.5%的伪装成常用程序与文件的恶意程序则是把自己伪装成了各种文档或文件。其中，伪装成办公文档（如 Office 文档、PDF 文档、WPS 文档等）的总量的约占 34.9%，

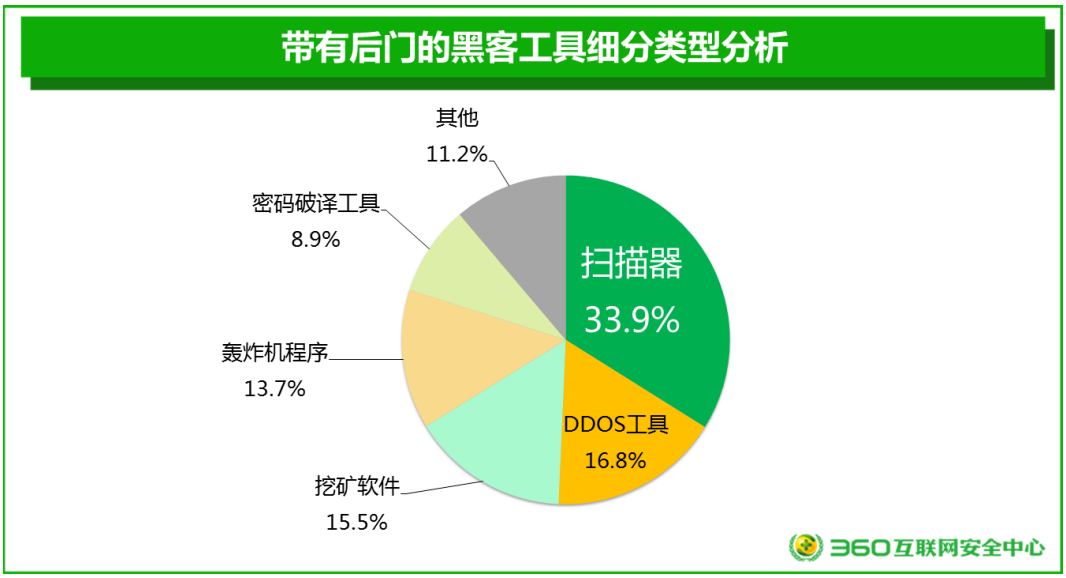
伪装成压缩包的约占 17.1%，伪装成图片的约占 4.5%。



特别值得一提的是，伪装成各种文档或文件的恶意程序，常常会通过电子邮件进行传播，它们往往会用令人感兴趣的标题，以及精心设计，以假乱真的图标，来吸引受害者打开这些邮件附件。在普通的民用攻击中，这些文件很可能是敲诈者病毒，而在高级持续性攻击中，即 APT 攻击，这些程序则很有可能是特定组织精心设计的间谍软件。

六、 带有后门的黑客工具

黑客工具是指那些被用来寻找系统漏洞，窥探系统数据，制作木马病毒的非法工具。很多黑客或技术人员会通过论坛和搜索引擎找到并使用这些黑客工具。但实际上，目前网上流传的各种黑客工具，大多内置了后门或捆绑了木马。而使用这些黑客工具的人，在试图攻击他人的同时，自己也成为了他人攻击的目标。



统计显示，所有带后门的黑客工具中，扫描器排名第一，占比高达 33.9%。此类工具类型众多，常被用于网络渗透和漏洞检测，是很多黑客初学者的必备工具。其次是 DDOS 工具占比 16.8%；轰炸机占比 13.7%，挖矿机占比 15.5%，密码破译工具占比 8.9%。

第三章　2016 最具欺骗性的恶意软件实例

一、　TOP1 传奇依旧之游戏外挂

欺骗指数：★★★★★

危害指数：★★★★☆

清除难度：★★★★☆

“无热血，不江湖，无兄弟，不传奇”，如果你是一个资深的传奇游戏爱好者，你一定不会感到陌生。

游戏作为互联网娱乐性应用的代表，因其丰富的游戏内容、代入感强、拥有社交属性等特点，已经成为大多数网民日常生活中不可或缺的重要组成部分。正因用户基数巨大，这给私服外挂带来巨大的市场，特别是针对一些热门游戏的外挂，如 LOL、DNF、传奇私服等。然而，部分私服外挂存在着恶意推广，捆绑木马远控等行为。

下面是一款热血传奇私服外挂的实例。我们通过分析该私服外挂，发现程序中有一个博客的网址。从这个博客上可以看到该私服访问量很大，说明这个私服已经有不少玩家。仔细看看，这个博文表面上是一些乱打出来的字符串，其实这是一段加密的数据，解密出来则是一个 IP 地址和端口。私服登录器在运行时会连接该地址下载文件， 该文件是完全可以由作者自由更换，这种利用博客进行云控的方式在私服外挂中使用非常广泛。

在此我们建议广大用户谨慎使用私服登录器以及相应的外挂，一旦运行这些私服外挂，你的电脑很可能就会沦为“肉鸡”，任由黑客摆布。

二、 TOP2 天上掉馅饼之贪便宜软件

欺骗指数：★★★★☆

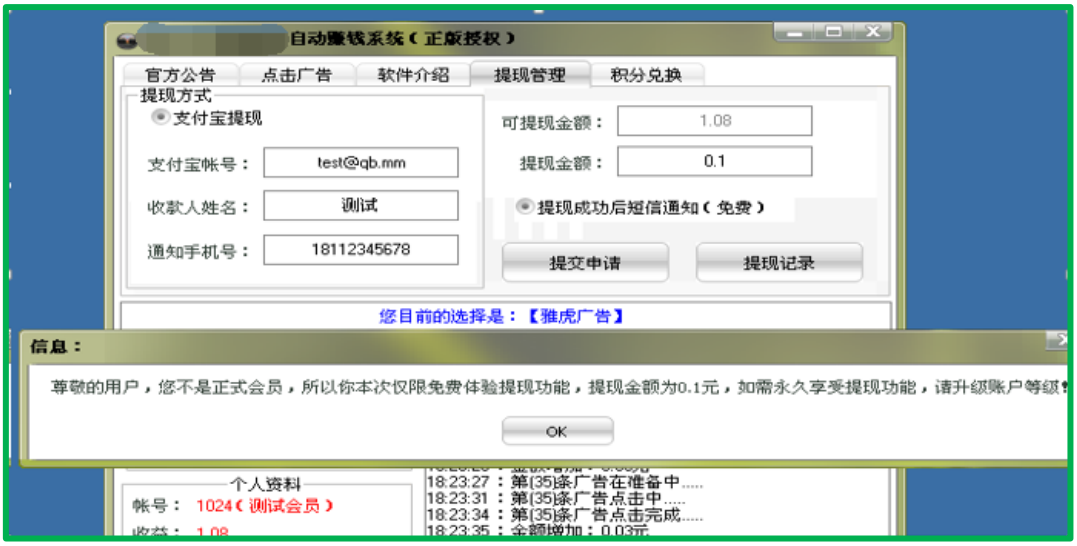
危害指数：★★★☆☆

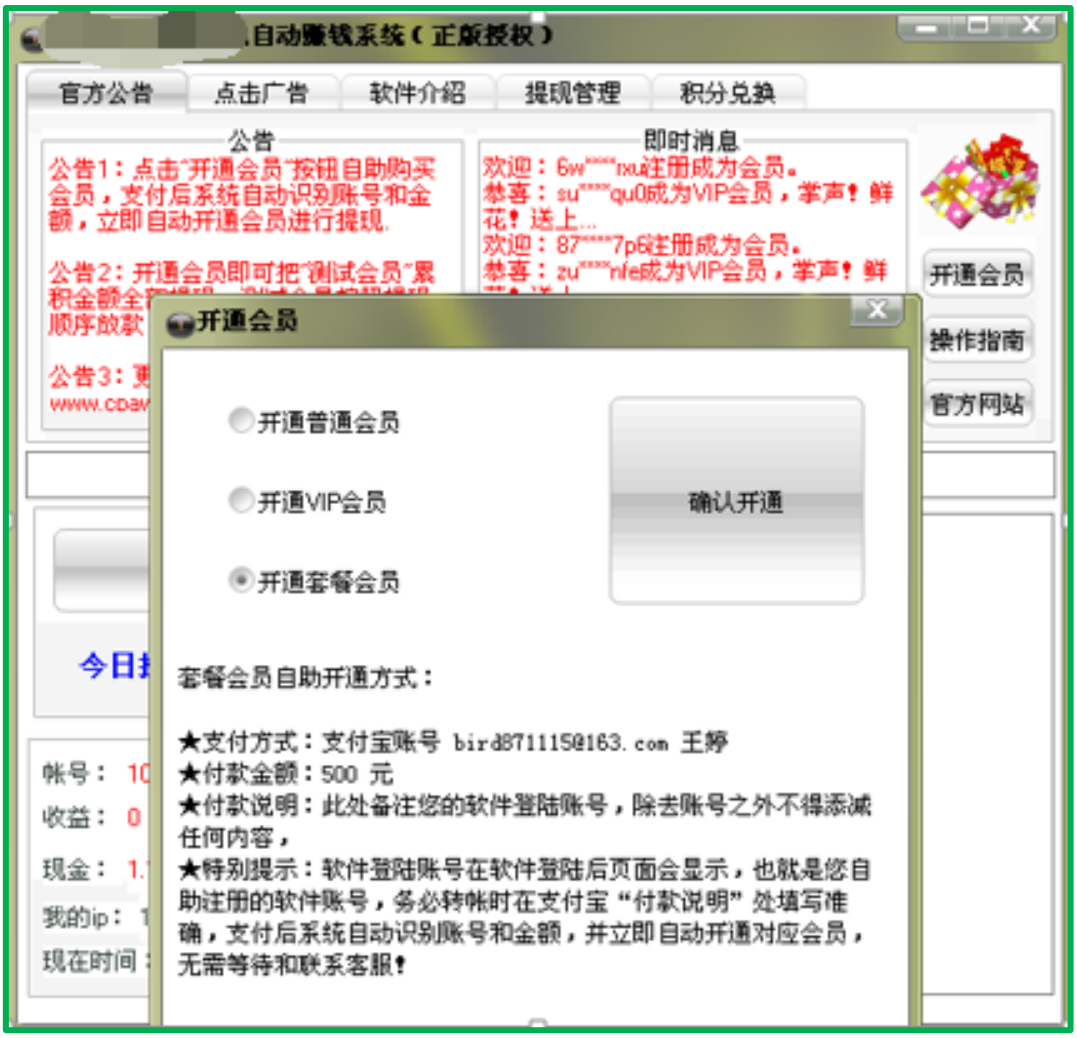
清除难度：★★☆☆☆

天上掉馅儿饼这种事儿，是做梦都会笑醒的！现如今网络上的虚假软件随处可见，已成为主要危害之一，这些软件抓住部分用户贪便宜的心态，从而得到快速传播。例如部分用户觉得网赚很爽，不用风吹日晒，电脑上运行这个软件，就能把钱赚到手，实际上这类恶意软件有的是欺骗用户充值，有的是伪造网银、支付宝等页面进行钓鱼盗号。又如领话费、流量等工具，此类软件一般是利用其他网站举办活动的验证缺陷进行领取，但是实际上绝大多数网站都会第一时间修复漏洞，所以基本上能够见到的此类软件都因漏洞被修复或者活动结束而无法领取，当用户实际上在计算机上运行了此类软件，往往不但没有领取到话费，反而浏览器首页会被莫名其妙锁定到各种导航网站，或者桌面上突然多出几个静默安装程序的图标，真是赔了夫人又折兵，便宜没占到，反而被人暗算一把。

下面以一款名为“XX 挂机自动赚钱系统”的软件为例，用户注册并运行这类软件之后，首先看到的是软件界面是显示的一系列的“XX 提取的 XX 元现金”，“XX 升级成为 VIP”等提示语，然后点击开始赚钱之后，发现账户上的钱在唰唰唰的往上涨，好像真的什么都不需要做，只需要让它安静的运行即可赚钱。赚了钱自然就得提现，用户提现的时候，恶意软件作者邪恶的爪牙就显露无遗了，叮！“你只能提现 0.1 元，如果想提取全部的金额请升级为 VIP”，怎么升级 VIP 呢？充钱！没错，这就是它的套路，通过此种方式来骗取用户充值。

遇到这种情况，请大家谨记，天上不会无缘无故掉馅饼!





三、 TOP3 色字头上一把刀之色情播放器

欺骗指数：★★★☆☆

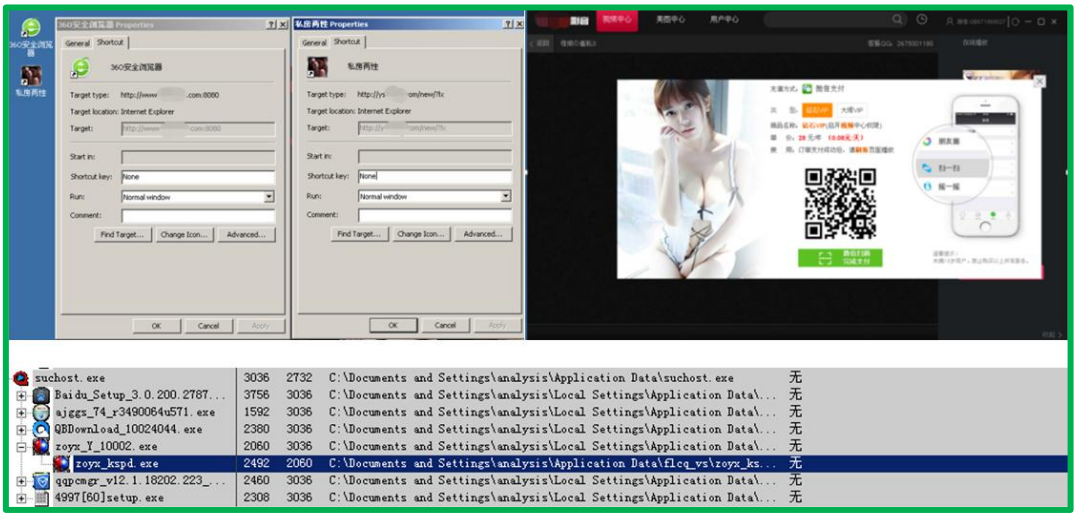
危害指数：★★★★☆

清除难度：★★★☆☆

网络上充斥着各种诱惑，恶意软件作者就特意瞄准了这群按耐不住洪荒之力的小伙伴们，借此传播各种恶意软件。

这类恶意软件通常都有一个很具诱惑性的名字以及一个美女图标或快播图标，在使用过程中，大多都会有欺骗用户充值、静默安装推广软件、锁定浏览器主页、植入后门木马等行为，甚至有感染、勒索行为。

比如以下这款影音软件，一旦用户打开运行就会在桌面上生成伪装成 360 浏览器以及具有诱惑性名称和图标的恶意快捷方式，同时该软件会通过云控下载并安装各种推广大礼包，其中充满各种让人把持不住的诱惑性图片，如果想观看就需充值付款，软件作者通过这种套路来欺骗用户充值牟利。



四、 TOP4 放纵不羁爱自由之恶意破解软件

欺骗指数：★★★☆☆

危害指数：★★★☆☆

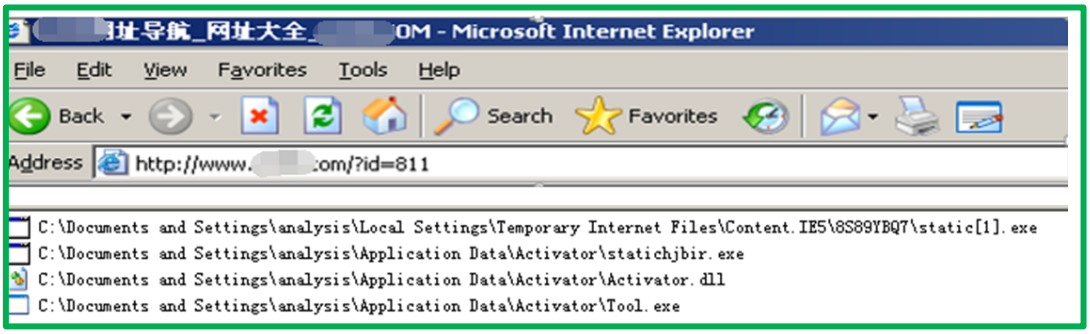
清除难度：★★★☆☆

随着现在网络的迅猛发展，提供各式各样服务的软件层出不穷，其中很多软件提供给普通用户的都有一定的功能限制，特别是专业的行业软件，只有支付一定的费用，用户才能使用更高级的功能，软件收费本身是无可厚非的，但是对于有些用户来说，更愿意去寻找免费的破解版本使用。

很多恶意软件作者正是抓住了用户这点心理，打着“XX 破解版”、“XX 激活软件”等旗号，静默安装推广软件，甚至植入后门木马进行远控等行为。

例如下面这款系统激活软件，当用户点击“激活”按键时，该软件会设置默认主页进行推广，并且修改开始菜单（C:\Documents and Settings\analysis\Start Menu\Programs）中 Internet explorer 快捷方式，使其指向推广链接。同时，软件还会连接远程地址下载恶意文件到 IE 缓存目录中，达到控制用户电脑的目的。

因此，用户在激活时，尽量选择正版序列号进行激活，以防止自身电脑中毒。



五、 TOP5 披着羊皮的狼之伪装文件

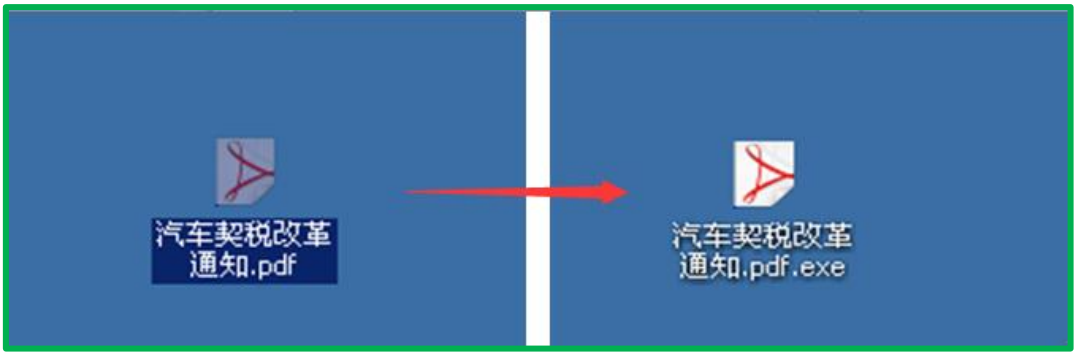
欺骗指数：★★☆☆☆

危害指数：★★★★★

清除难度：★★★★☆

恶意软件中一直存在这么一种手段简单但中招率高的手法，就是将可执行文件图标伪装成 doc，pdf，xls，rar 等文档文件或者其他正常软件。这类软件的名称都是经过精心伪造，伪装成用户感兴趣的名称，降低用户警惕，诱使用户直接运行。

就如下面这个恶意软件，它将可执行文件图标伪装成 pdf 图标，如果用户设置文件选项中的隐藏文件的后缀名，它显示的名称将是“汽车契税改革通知.pdf”，其实它的真实文件名为“汽车契税改革通知.pdf.exe”，这个恶意软件其实是一个敲诈者，一旦得以运行将会加密磁盘内的所有文档，用户只有按照提示支付比特币才有可能获得解密。



又如下面这些文件，实际上都是具有远控性质的恶意代码，而并非真正的图片或 WORD 文件。

六、 TOP6 骇客帝国之黑客工具

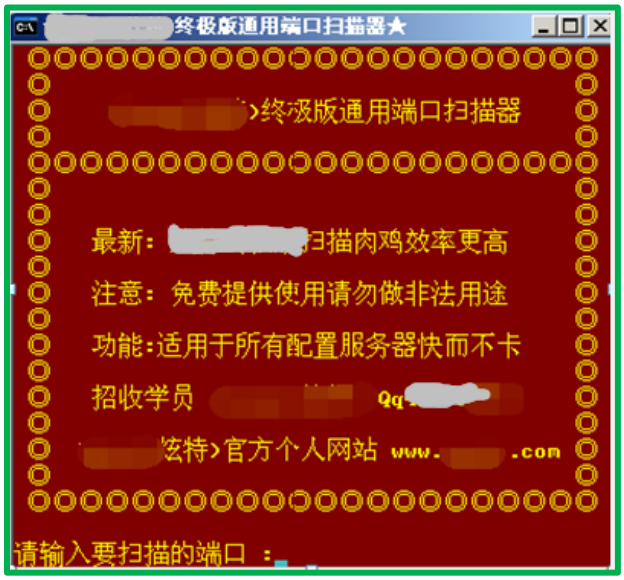
欺骗指数：★★☆☆☆

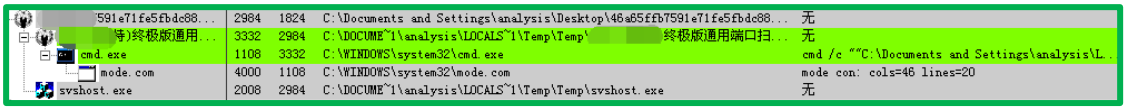
危害指数：★★★☆☆

清除难度：★★★★☆

在常人的眼中，黑客只需轻敲几下键盘，就能控制对方电脑。这也间接导致了部分用户想学各种黑客技术用于获取非法信息，来满足自己的虚荣心。部分初学者都只是简单的使用互联网上现有的黑客工具来达到目的。如端口扫描、社工辅助、挖矿机等工具。这些工具很多都包含恶意行为，如静默推广、捆绑木马病毒等，导致很多用户蒙受欺骗。

例如下面这款端口扫描软件，当用户点击运行时，还没有任何操作，该程序就会在临时目录（C:\Documents and Settings\user name\Local Settings\Temp\）释放恶意程序 svshost.exe 并运行，该程序实际为远控木马，用户还未攻击别人时，就已沦为别人的“肉鸡”，任由摆布。





因此，请用户尽量不要使用来源不明的黑客工具，否则还未攻击别人，自己已中招。