勒索软件“假面”系列——代刷软件



2018年4月02日

目 录

[第一章 勒索中的“代刷” 1](#_Toc510097438)

[一、勒索软件伪装类别分布 1](#_Toc510097439)

[二、主流的伪装类别——代刷软件 1](#_Toc510097440)

[第二章 代刷软件 3](#_Toc510097441)

[一、定义与分类 3](#_Toc510097442)

[二、来源 3](#_Toc510097443)

[三、实现原理 3](#_Toc510097444)

[四、示例 5](#_Toc510097445)

[第三章 代刷产业分析 7](#_Toc510097446)

[一、角色分工 7](#_Toc510097447)

[二、推广与盈利 7](#_Toc510097448)

[三、用户群分析 9](#_Toc510097449)

[四、相似的平台架构 10](#_Toc510097450)

[五、加速移动化 12](#_Toc510097451)

[第四章 代刷软件的危害 14](#_Toc510097452)

[一、代刷暗藏“杀机” 14](#_Toc510097453)

[二、统一治理 15](#_Toc510097454)

[总结 17](#_Toc510097455)

[360烽火实验室 17](#_Toc510097456)

第一章 勒索中的“代刷”

勒索软件是指启动后通过置顶自身窗口或重置锁机密码强制锁定用户桌面、使用户无法正常使用设备，并以支付解锁对用户进行勒索的软件。近年来，Android平台勒索软件以其高危害、高伪装性、难卸载等特点一直是360烽火实验室关注的重点。针对勒索软件擅于伪装成特定流行软件进行传播的现象，360烽火实验室对Android平台勒索软件伪装类别及相关产业进行了持续跟踪与分析。在2018年3月初发表的《勒索软件“假面”系列——免流软件》中，我们已经介绍了勒索软件的一类“假面”——免流软件，并对免流产业现状、原理与危害做了详细阐述。近期，我们把目光瞄准了一类比免流软件更加常见的伪装类别——代刷代挂类软件（以下简称代刷软件）。

## 一、勒索软件伪装类别分布

从勒索软件伪装类别分布情况可以看到，勒索软件伪装类别以色情和黑客工具为主，而在黑客工具中，代刷类占比位列第二，仅次于外挂、辅助类。

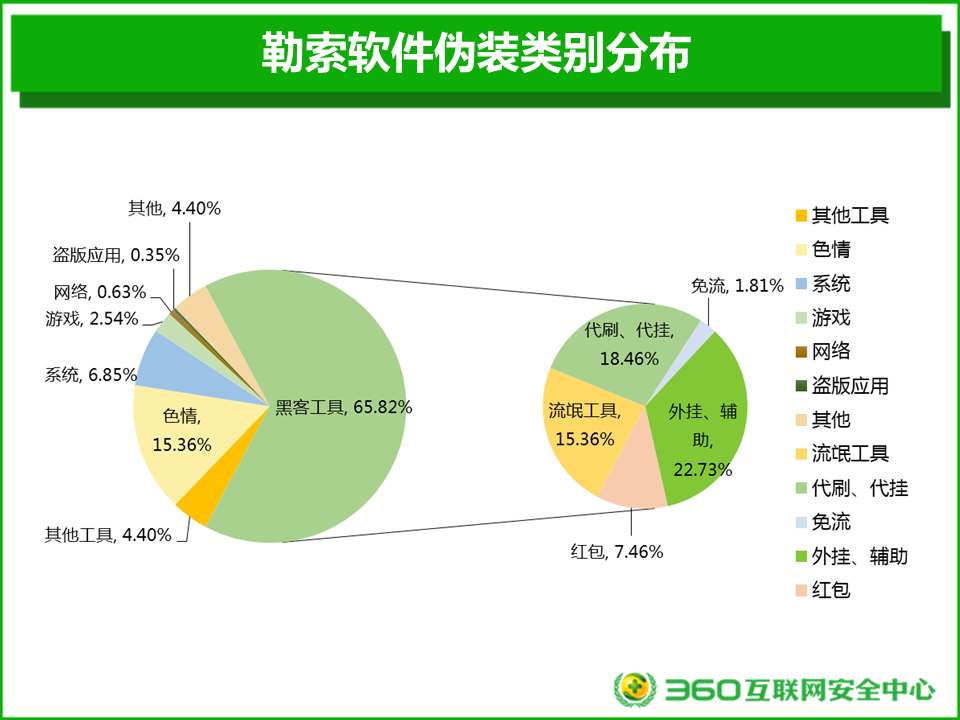


图1.1 勒索软件伪装类别分布

## 二、主流的伪装类别——代刷软件

伪装成代刷软件的勒索软件名称多为“XX代刷”、“XX代挂”或“XX业务”，实际运行后会置顶特定窗口阻止用户进入桌面，或者申请设备管理器锁屏密码相关权限并在用户授权后实施锁屏。



图1.2 冒充代刷软件的勒索软件

截止到2018年3月，360烽火实验室共捕获到超过20万个代刷软件，其中恶意勒索软件占比高达57.4%，这些软件打着代刷、代挂的幌子诱导用户下载、安装或激活设备管理器，随后对用户进行锁屏勒索，给用户设备与财产安全带来了严重威胁。

大量勒索软件伪装成代刷软件传播充分反映了代刷软件拥有着可观的市场空间。实际上，随着近两年来移动社交软件与视频直播软件的流行，越来越多的用户开始关注自身账户等级、特权、以及粉丝量等指标，以少量金钱、时间换取高账户特权等级、高粉丝量成为了部分用户的强烈诉求，代刷软件由此“应运而生”并飞速传播开来。通过对代刷软件进行持续跟进与分析后发现，代刷软件以其价格低廉、功能齐全、兼容性强、操作简单、效果显著等特性吸引了大量商家与用户，且从商家最初建站到用户最终购买已形成了清晰的产业链。

第二章 代刷软件

## 一、定义与分类

代刷软件是指通过特定手段提高特定账户粉丝量、访问量或挂机时间等量化指标，或者获取特定权限的软件。常见的代刷软件可分为刷量、刷会员与代挂三种：

1. 刷量：即刷高特定账户量化指标，量化指标可细分为访问量、点赞量、评论量、转发量、粉丝量、分享量、播放量等；
2. 刷会员：即为特定账户刷取特权，将普通用户提升为特权用户，以QQ刷钻最为常见；
3. 代挂：即代理挂机，通过获取用户的登录凭证来代替用户登录与挂机。

## 二、来源

通过对大量Android代刷软件进行分析后发现，绝大多数代刷软件都是由Web代刷网站转化而来。目前市场上有很多Web网站打包工具与平台，例如AIDE、IAPP、E4A等开发工具以及变色龙、九维云打包等软件打包平台，利用这些工具或平台可以非常便捷地将特定Web网站转换成对应的代刷软件，且转换出来的代刷软件具有十分相似的文件清单与代码架构。代刷软件开发者只需要提供代刷接口与不同的软件名称，即可快速生成多款代刷软件。

我们对捕获到的代刷软件开发工具进行了统计与分类，由统计结果可以看到，开发工具开发出的代刷软件数量远大于Web打包平台打包生成的代刷软件数量，而在开发工具中，由AIDE、IAPP、E4A三类工具开发的代刷软件占比高达80%以上，其中AIDE最为常用。

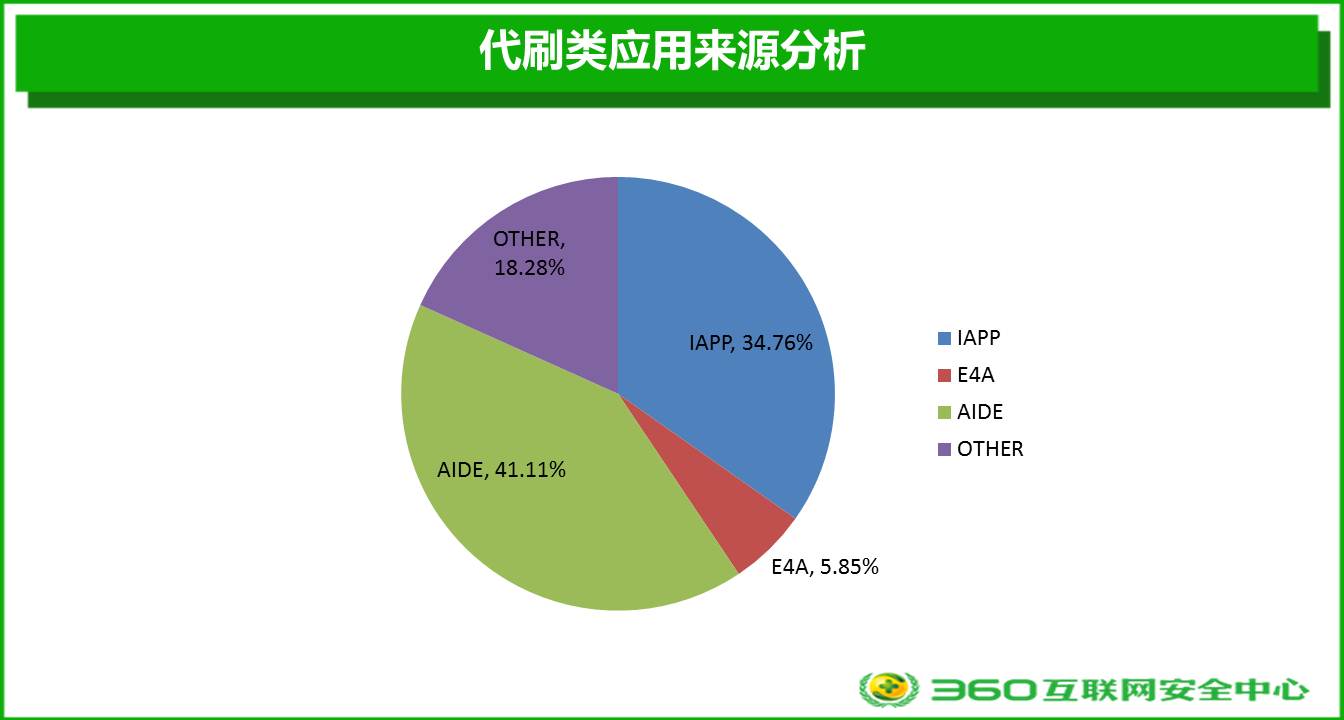


图2.1 代刷软件来源分析

简易开发工具与软件打包平台的普及很大程度降低了代刷软件的开发门槛与成本，在低门槛与低成本的诱惑下，不少代刷商家利用代刷软件的方式推广其代刷网站，并在移动端与Web端“双线”经营，极大提高了盈利效率。

## 三、实现原理

1. 代刷软件刷量原理

Web代刷网站的内容与源码十分简单，基本上只包含下单功能与订单处理逻辑。代刷软件实质与Web代刷网站一样，都只是一个为用户提供下单购买功能的下单平台，并不包含实际的刷量逻辑。用户通过代刷软件提交订单后，代刷软件会将订单请求传递至代刷网站，代刷网站随后在后台进行统一处理，并将刷量请求传递给真正实现代刷功能的供货商代刷后台。

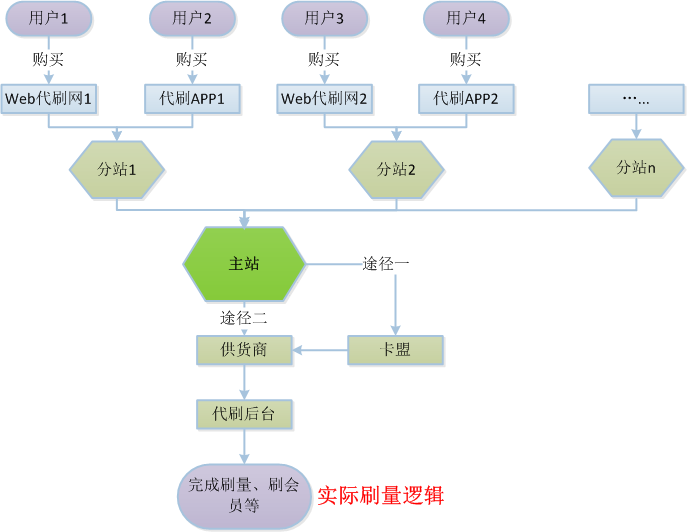


图2.2 代刷完整流程

1. 实际刷量逻辑

供货商的代刷后台是实际实现代刷逻辑与完成代刷业务的地方，而针对不同类型的代刷业务，代刷后台会应用不同的代刷原理：

1. 刷量业务。

刷量业务通常是通过僵尸账号实现的。代刷逻辑开发者通过一定手段获取到海量僵尸账号，同时获取到官网的点赞、加粉丝、转发等接口，然后在服务器上搭建好一套控制僵尸账号自动化访问指定接口的代刷系统就可以进行自动的刷量操作。除了利用僵尸账号，目前还存在另一种刷量方式，即将有刷量需求的用户通过共同的平台聚集到一起，这些账号之间通过人工互刷可以达到真人刷量的目的。真人刷量的代表软件有“快手网红联盟”，这是一款只支持为特定应用刷量的软件，使用此软件的都是真实用户，这些真实用户间通过互相浏览、点赞或评论等操作来增加彼此的浏览量、点赞量或评论量等量化指标。



图2.3 某手网红联盟

1. 刷会员。

刷会员业务通常是通过不正当利用运营商计费机制实现的。与免流软件实现原理一样，刷会员业务也是利用了运营商代理系统与计费检测系统分离的特点，通过特定手段使得这两个分离的系统对购买结果处理不同步，从而达到廉价刷会员的目的。以刷QQ会员为例，这种“特定手段”通常是低价在淘宝等市场购买廉价SIM卡，然后用手机话费开钻后在一定的时间差内发送取消指令或者停机来干扰扣费结果。这种对运营商扣费结果的干预会导致运营商代理系统上显示绑定QQ的手机号购买了QQ会员等业务，而在运营商的计费检测系统上却没有购买后的扣费成功记录，以此达到免费订购QQ会员的效果。然而需要留意的是，这种代刷手段存在一个问题——无法长期维护会员状态，开通期限最多一个月。与刷量相比，刷会员业务用户承担的风险比较大，不仅刷入会员的期限无法保证，而且还面临被封号的风险。

1. 代挂。

代挂的原理较前两种业务简单，即通过用户的登陆凭证登录用户账户并代替用户完成软件挂机。与前两种业务相比，代挂商家必须首先获取到用户的登录账号和密码，因此用户难免会面临账号密码泄露的巨大风险。

## 四、示例

Android代刷软件只是一个下单平台，逻辑十分简单。以一款由E4A工具开发的代刷软件为例，其核心代码如下图所示。该代刷软件会根据用户在下单交互界面所选择的业务类型、商品类型、数量等构造请求参数串，并通过特定请求接口将请求参数串发送到代刷网站。



图2.4 代刷软件核心代码

代刷网站也是一个下单平台，且交互界面与代刷软件十分相似。代刷网站在接收到代刷软件发送过来的业务请求后会将业务请求连同请求参数一同发送给代刷后台，代刷后台会根据请求参数完成代刷业务。

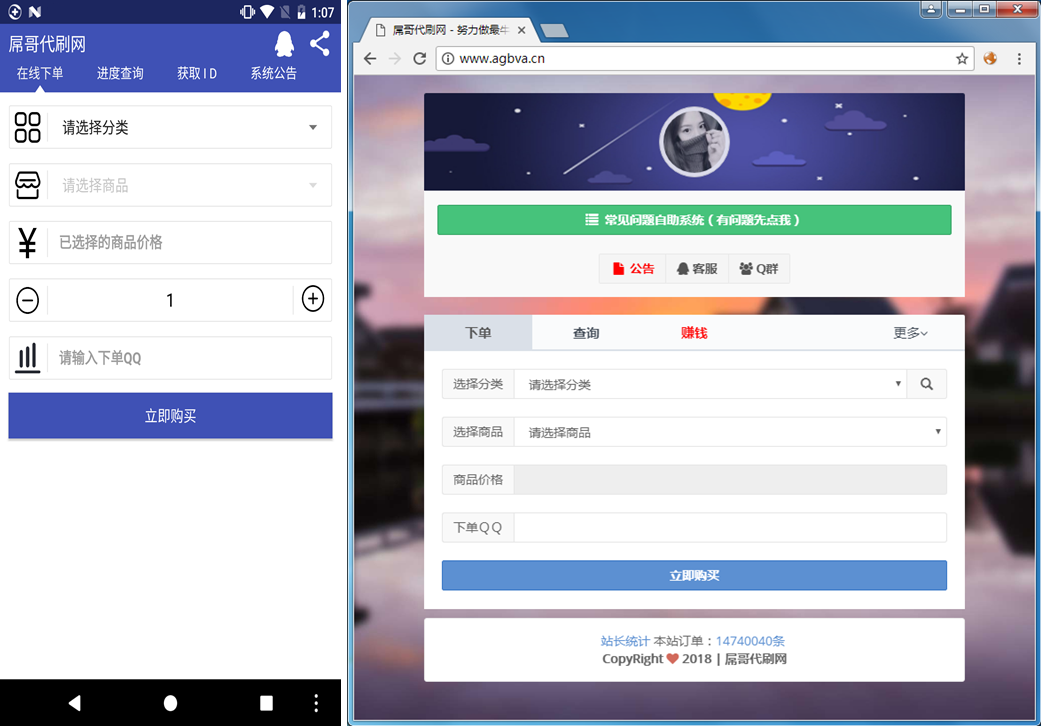


图2.5 代刷软件与对应的代刷网站

第三章 代刷产业分析

## 一、角色分工

与免流产业一样，代刷产业也形成了由上至下、层层发散的产业链，从最上层供货商到中间的各类主站、分站再到最终消费的用户，各角色间既各司其职又有功能衔接与交叉，共同维系着整个代刷产业。

1. 供货商。供货商作为代刷最上游，负责为下层主站提供代刷逻辑与业务支持。当收到主站发送过来的代刷请求时，供货商在自己的代刷后台应用代刷逻辑完成代刷业务并将业务结果反馈给主站；
2. 主站。主站是代刷产业的核心，其上游对接供货商或卡盟，下游对接各个分站，提供了数据存储、建分站、订单查询、支付等多种功能；
3. 普通分站。除了不能建立下级分站，普通分站几乎拥有和主站一样的功能。普通分站拥有修改网站公告、网站名字、网站logo、商品价格等权限。用户在分站下单成功后，分站管理员可以得到相应提成；
4. 高级分站。高级分站是普通分站的升级版，与普通分站不同的是高级分站支持开通下级分站，用户在高级分站或其下级分站上下单成功后高级分站管理员都可以拿到提成；
5. 用户。用户作为代刷最下游，无论是通过代刷软件消费还是Web代刷网站消费，最终都以购买代刷服务的形式为整个代刷产业的运作提供了资金来源。

## 二、推广与盈利

代刷产业是一种十分依赖于推广扩散来盈利的产业，一方面，在商家泛滥的代刷市场，推广程度会影响商家知名度，而知名度会直接影响用户数量；另一方面，主站与高级分站会从下级分站的收益中抽成，由主站与高级分站扩散出的下级分站越多，其收益越高。代刷产业也是一类“一本万利”的产业，只要维护好特定网站就可以不断推广获利。

1. 推广模式

代刷产业的推广呈现从主站由上至下层层扩散的架构，这是由代刷产业“上层吃下层回扣”的盈利模式决定的。首先，主站的经营者为了盈利，会将自己的代刷网站或者软件通过QQ群、论坛、贴吧等方式发布到网上进行推广，用户可以在这些网站下免费或者低价建立高级分站，成为高级分站管理员，高级分站管理员为了获取更多利益，也会用网络发布的形式去推广自己的分站，以此吸引用户购买代刷业务或在自身分站下建立低级分站，低级分站直接对接代刷业务消费用户，又再次通过网络发布对外推广自己的分站以吸引更多用户来消费。在这种模式下，代刷网站的下级分站与用户数目越多，网站的收益就越高。

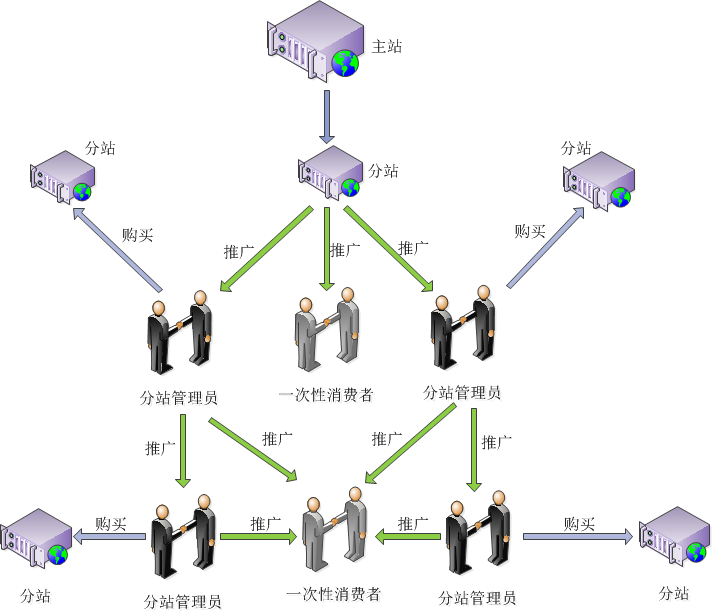


图3.1 代刷产业推广模式

1. 盈利情况

代刷业务以价格低廉的特点吸引了大量用户，而实际上，代刷走的是“薄利多销”的路线，再加上代刷网站或软件的开发与维护成本极低，一个流行代刷主站的获利往往十分可观。通过长期跟进多个流行主站与分站，我们整理汇总出了部分代刷网站的盈利情况。由图可见，主站的日平均利润在数十元至上千元不等，差距甚是悬殊。日均收益最高的是一个主机名为“qqdzz.com”的主站，其运营天数不到一年，而累计交易额已达到了一百多万。

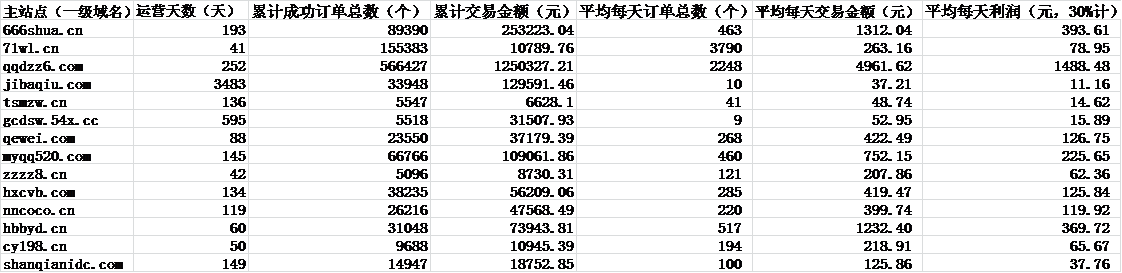


图3.2 部分代刷网站收益情况



图3.3 分站内部价格表

代刷分站可以自定义销售价格，但是由于代刷商家众多，各商家之间存在价格牵制，代刷业务的价格并不会有太大波动且十分低廉，因此一直吸引着广大用户消费购买。这种双方“各取所需、互利共赢”的模式使得代刷产业从产生到现在经久不衰。也正是因为如此，勒索软件的作者将矛头指向代刷这块“肥土”，以此来加速勒索软件传播与扩大勒索软件感染范围。

## 三、用户群分析

通过对TOP代刷QQ群成员分布分析发现，代刷产业的关注人群普遍偏年轻化，其中00和90后占据了半壁江山。虽然主站和高级分站会吃普通分站的提成，最后到普通分站的利润会大打折扣，但建立代刷分站销售代刷服务的赚钱渠道和很多传统赚钱渠道比起来成本低、耗时少且风险较小，因此这种业余赚钱渠道受到了不少初高中生以及大学生的追捧。



图3.4 代刷QQ群人员分布

此外，我们通过在代刷网站购买某知名直播平台的刷粉丝业务并在粉丝量大幅提升后，对这些“买来的”粉丝及其所粉的人群进行观测，这些“买来的”粉丝在关注购买者的同时也关注了很多其他的用户，其中不乏一些在直播平台排名靠前的主播，这说明现在流行直播平台上的某些大主播也有“买粉”嫌疑。随着网络社交与直播平台的风靡，不少用户出于攀比心理或扩大自身知名度与影响力的原由，可能会迫切追求高粉丝量、高评论数等量化指标，而代刷业务就“雪中送炭”成为了他们的最佳选择。

## 四、相似的平台架构

通过对几个流行代刷网站的分析发现，虽然这些代刷网站的网址不同，但网站上的内容以及功能都大同小异。对这些代刷网站进行抓包后的结果显示，它们的组织结构、网络请求和返回值字段大体相似，例如注册分站的URL都包含一个共同的路径（/user/reg.php），且获取QQ说说的请求URL也大体相同。

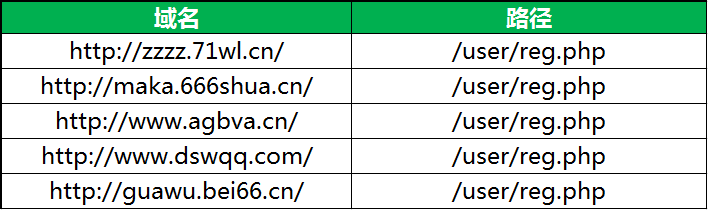


图3.5 注册分站的URL列表

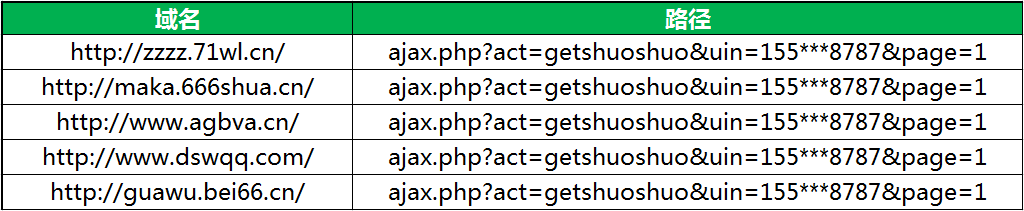


图3.6 获取说说的请求URL列表

通过进一步分析从网络上随机取得的建站源码中包含的注册分站和获取QQ说说的代码，我们发现此源码结构及代码功能和这些代刷网站的源码与功能极其相似。由此基本可以判定市面上的代刷网站大部分都是使用的同一套建站源码。通过这套源码，建站者只需拥有自己的主机和域名就可以轻松建站，能力要求与成本极低。代刷产业正是凭借着低成本与门槛吸引了众多兼职人员加入其中。



图3.7 建站源码结构



图3.8 建站源代码

## 五、加速移动化

现今，移动互联网的发展势头正在渐渐超越传统互联网，面对移动互联网这块“肥肉”，代刷产业的步伐也没有停歇，代刷主战场已逐渐从Web平台转移到移动代刷软件。自2015年开始，Android代刷软件开始批量出现并逐渐增多，且近几年增长趋势逐年增强，仅2017年一年新增的代刷软件就超过了15万个，是2016年总量的3.1倍、2015年总量的35.6倍。

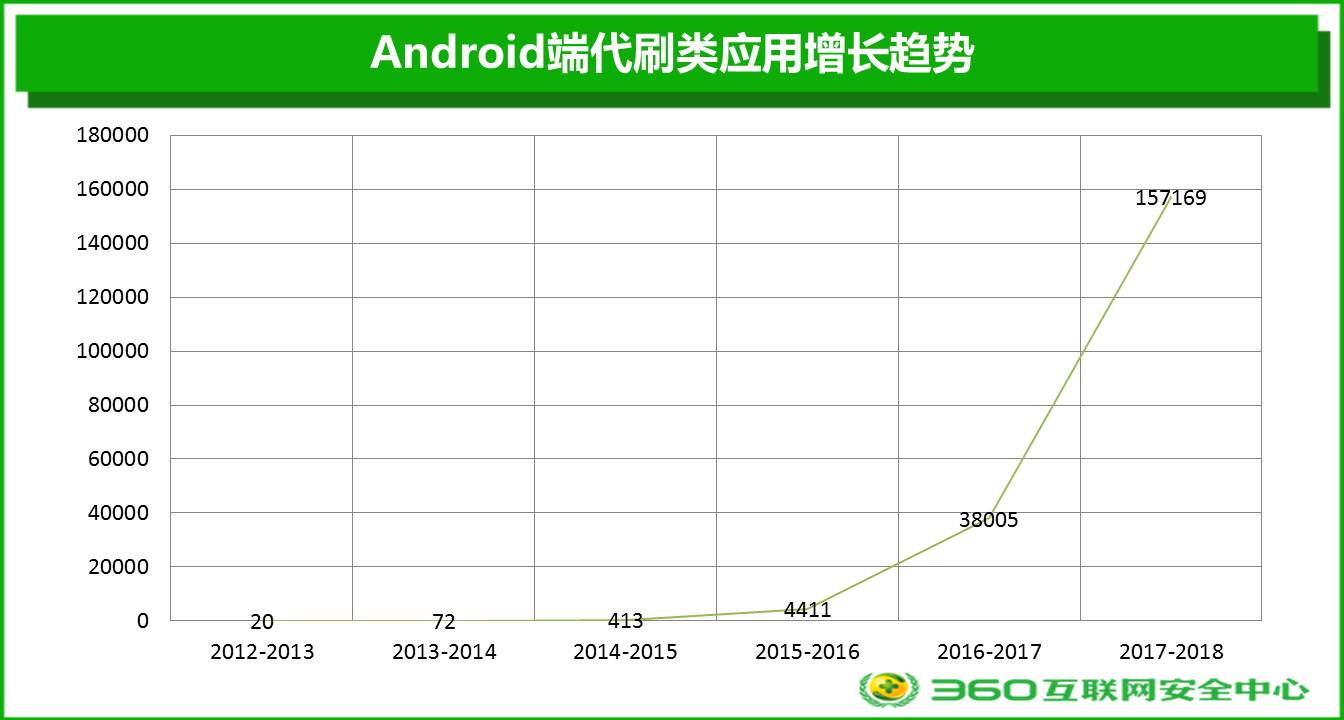


图3.9 Android代刷软件数量增长趋势

近年来，随着各种Web转手机软件厂家的增多，生成一个手机软件的成本几乎为零。代刷软件的流行给代刷产业带来了又一次春天，但同时代刷市场鱼龙混杂、良莠不齐，一些不法分子打着代刷的旗号传播盗号、勒索等恶意软件，给用户带来了极大的经济损失。

第四章 代刷软件的危害

## 一、代刷暗藏“杀机”

目前代刷软件中充斥着大量危险的仿冒代刷软件，它们打着代刷的旗号，在用户安装后实施勒索、盗号等恶意行为，给用户隐私与财产安全带来了严重隐患。

1. 锁机勒索

在我们捕获到的代刷软件中，超过一半是恶意锁屏勒索软件。用户在下载安装代刷软件时，极有可能上了勒索软件的钩，而由于代刷软件本身并不是一种合规软件，这些受害用户在被锁屏勒索后，很有可能会选择妥协并主动支付解锁，这越发助长了勒索软件开发者的嚣张气焰与利用用户侥幸心理实施犯罪的行径。

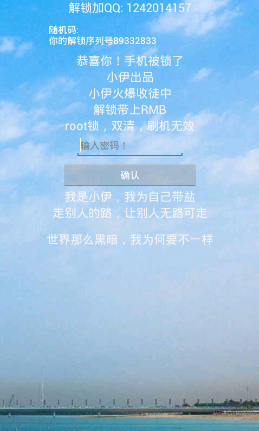


图4.1 仿冒勒索软件的代刷软件

1. 账号、密码被盗，通讯录被窃

盗窃账号、密码的行为多出现在由IAPP、AIDE等工具开发的恶意代刷软件中。这类软件最明显的特点就是在软件启动后出现账号、密码输入界面，并以代刷诱导用户输入账号与密码，一旦用户点击确认登录按钮，所输入的登录信息就会以短信或网络的方式被发送到指定手机或服务器上。这类软件属于欺诈盗号木马且实际上没有代刷功能，用户不但不能达到代刷的目的，反而会造成自己的账号密码被盗。

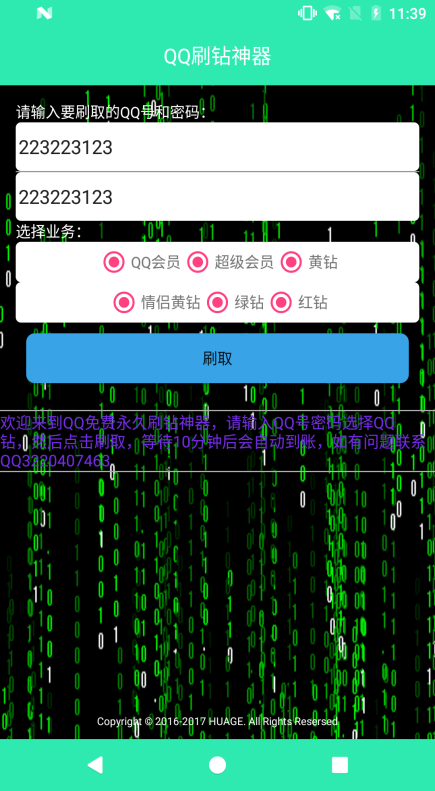


图4.2 盗号界面

除了盗取用户登录凭证，恶意代刷软件还“热衷于”窃取用户的短信、联系人、通话记录等隐私信息。这类代刷软件一旦被安装，会自动获取用户短信、联系人、通话记录等信息并通过各种方式（短信、邮件、网络）上传到远程服务器，且多数情况下，这些软件在首次启动后会自动隐藏桌面图标，使得用户日常无法感知且无法正常卸载，以此达到长期潜伏、持续作恶的目的。

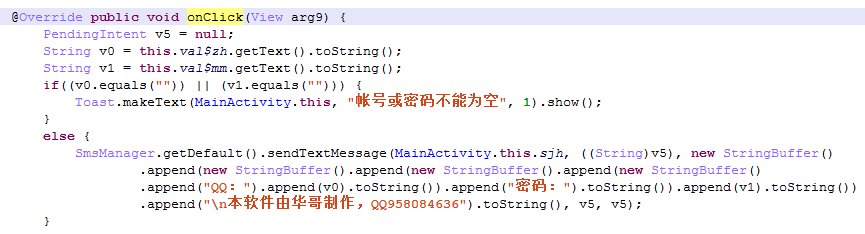


图4.3 发送短信的代码

1. 变相诈骗

部分代刷软件由于技术落后、端口被封杀等原因无法实现正常的代刷功能，但是其运营人员仍大量推广出售此代刷业务，用户在充值后非但不能实现代刷，充值的金钱也无法退回。这类变相诈骗防不胜防，给用户财产安全带来了严重威胁。

## 二、统一治理

2018年1月份，北京网信办针对网络上存在的热搜榜、热门话题榜等的刷榜行为进行了统一治理。在对相关负责人进行了约谈后，于2月2号发布了《微博客信息服务管理规定》，开始对微博客信息服务进行更严格监督与管理。



图4.4 网信办发布《微博客信息服务管理规定》

刷榜行为制造的虚假信息扰乱了社会秩序、损害了公共利益、扭曲了社会道德风向，有的甚至还会带来直接的经济损失。代刷软件作为实现刷榜的一类工具亟待治理，以此还公众一个真实、公平的网络空间。

总结

代刷本身是一个游离于制度边缘的产业，代刷用户都是抱着侥幸或者虚荣的心理进行尝试。恶意软件开发者正是利用了用户的这种心理，大肆传播仿冒代刷软件的恶意软件。随意下载安装与使用代刷软件可能会给用户带来不可预知的风险，对此，用户需要注意：

1. 尽量避免使用不合规软件；
2. 尽量在正规应用市场下载应用，不要轻易安装各种聊天群或论坛的软件；
3. 谨慎授予软件设备管理器等高风险权限；
4. 安装安全防护软件，以便及时识别恶意应用，确保设备与财产安全；
5. 一旦手机中毒，请及时联系移动安全厂商，以最大程度地减少损失。

360烽火实验室

360烽火实验室，致力于Android病毒分析、移动黑产研究、移动威胁预警以及Android漏洞挖掘等移动安全领域及Android安全生态的深度研究。作为全球顶级移动安全生态研究实验室，360烽火实验室在全球范围内首发了多篇具备国际影响力的Android木马分析报告和Android木马黑色产业链研究报告。实验室在为360手机卫士、360手机急救箱、360手机助手等提供核心安全数据和顽固木马清除解决方案的同时，也为上百家国内外厂商、应用商店等合作伙伴提供了移动应用安全检测服务，全方位守护移动安全。