StealthBot：150余个小众手机品牌预置刷量木马销往中小城市



****

2018年4月19日

## 主要发现

移动平台的流量黑产一直是我们的研究对象，2017年我们在《移动平台流量黑产研究——流量作弊与流量泡沫》报告中揭露了用于流量作弊的恶意刷量木马，该木马幕后指向北京的一家互联网服务公司。通过对该公司推广渠道的跟踪分析，我们发现了新型的刷量作弊木马家族，由于这类家族使用了特殊的自我隐藏方式以及成熟的模拟点击流程，如同一批由工厂自动流水线生产出来的隐形机器人，我们借用《刺猬索尼克》中一款隐形机器人的名称命名该家族为StealthBot。

根据我们的监测情况，StealthBot今年1月开始出现，截止到4月中旬，短短3个多月的时间里累计感染量超过400万，与一般的大规模感染情况不同的是，StealthBot感染的手机品牌多达150余个并且集中在小众手机品牌，感染地区避开了一、二线大城市主要集中在国内的中小城市。

StealthBot伪装成系统通知服务，它支持开机自动运行及外部唤醒等启动方式，运行后耗费用户数据流量，自动更新并加载最新版本的恶意插件，响应服务器下发的指令，完成涵盖搜索、购物、新闻、视频、红包等多个领域的刷量作弊推广功能。

在对StealthBot整个感染链的分析中发现，涉及到多家公司共同参与制作传播，我们监测到主要是通过供应链攻击的方式在用户使用手机前预置到这些小众品牌的手机系统中。

## StealthBot如何运行

StealthBot伪装成系统应用，并隐藏图标，接收指定的大量系统广播或者自定义广播启动。



图2.1 广播启动图

## 庞大的刷量业务范围

StealthBot会定时联网与服务器通信，更新并加载最新的SDK恶意插件，根据我们流量监测情况，短短3个月的时间里共更新了91个版本，频繁调整刷量功能及业务范围。

该插件通过接收与响应服务器下发指令，后台隐藏执行多种作弊刷量推广业务，进而实现自身牟利。目前最新版本的作弊刷量推广业务涵盖搜索、购物、新闻、视频、红包等多个领域。

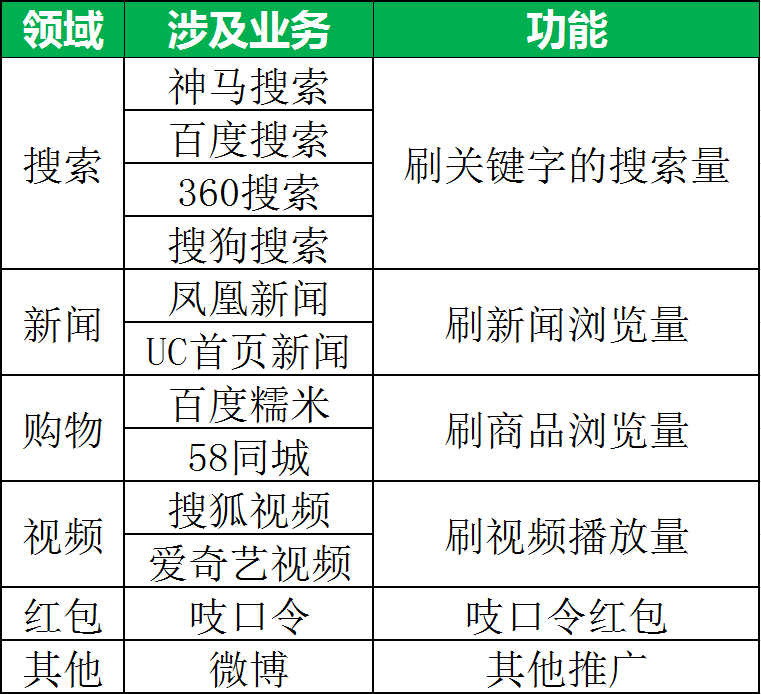


表1 最新版本的作弊刷量推广业务列表

## 巧妙的隐藏方式

与之前曝光过的刷量作弊木马隐藏方式不同，为了避免被用户发现，StealthBot采用了极为巧妙的隐藏方式，分别采用了人体感官视觉和听觉两种隐藏方式。

### 视觉隐藏——透明窗体

StealthBot使用透明且无焦点的WebView窗口覆盖正常的应用程序窗口



图4.1透明窗体代码片段

推广过程中用户看到的顶层界面和实际运行顶层界面请参考下面的模拟图



图4.2推广过程模拟图

### 听觉隐藏——页面静音

在遇到视频、动画等有声音的页面时，调用JavaScript脚本设置页面静音。设置静音行为在电信诈骗场景中较为常见，用于辅助窃取验证码短信信息和来电转移，在刷量木马上还是首次出现。

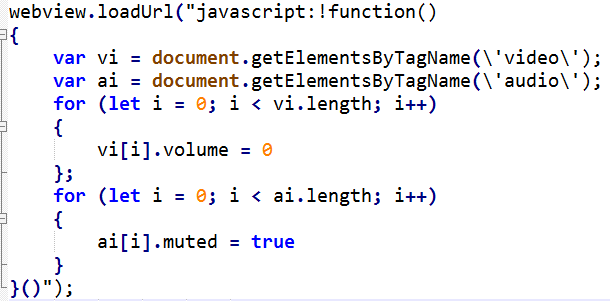
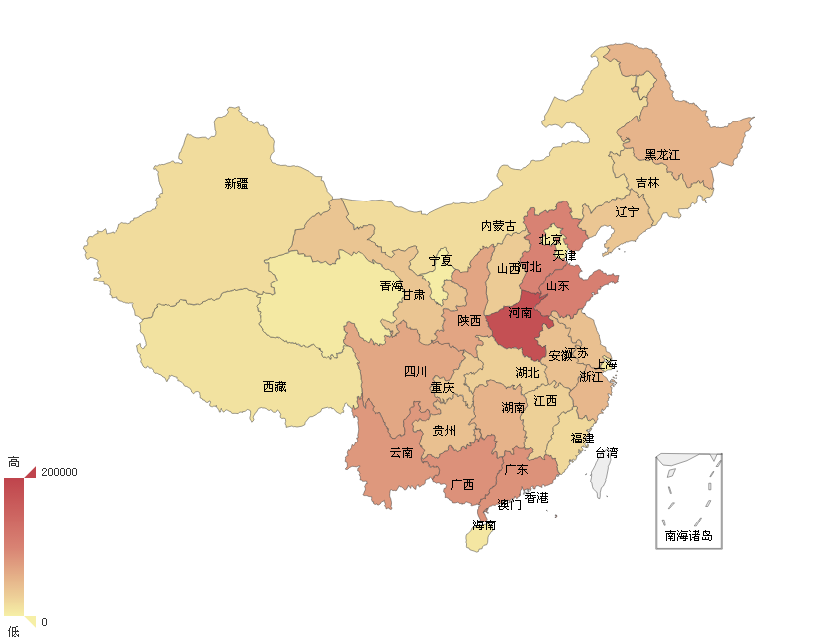


图4.3设置页面静音代码片段

在我们之前发的报告中总结过一些木马的逃逸技术，以上两种巧妙的感官隐藏方式是对木马逃逸技术的进一步补充。

## 中小城市、小众手机为主要目标

根据我们的监测情况，StealthBot今年1月开始出现，截止到4月中旬，短短3个多月的时间里累计感染量超过400万。

****图5.1国内感染分布情况

从感染省份来看，与常规木马不同的是，广东、北京并非此次事件的重点灾区。河南、山东、河北位列前三。

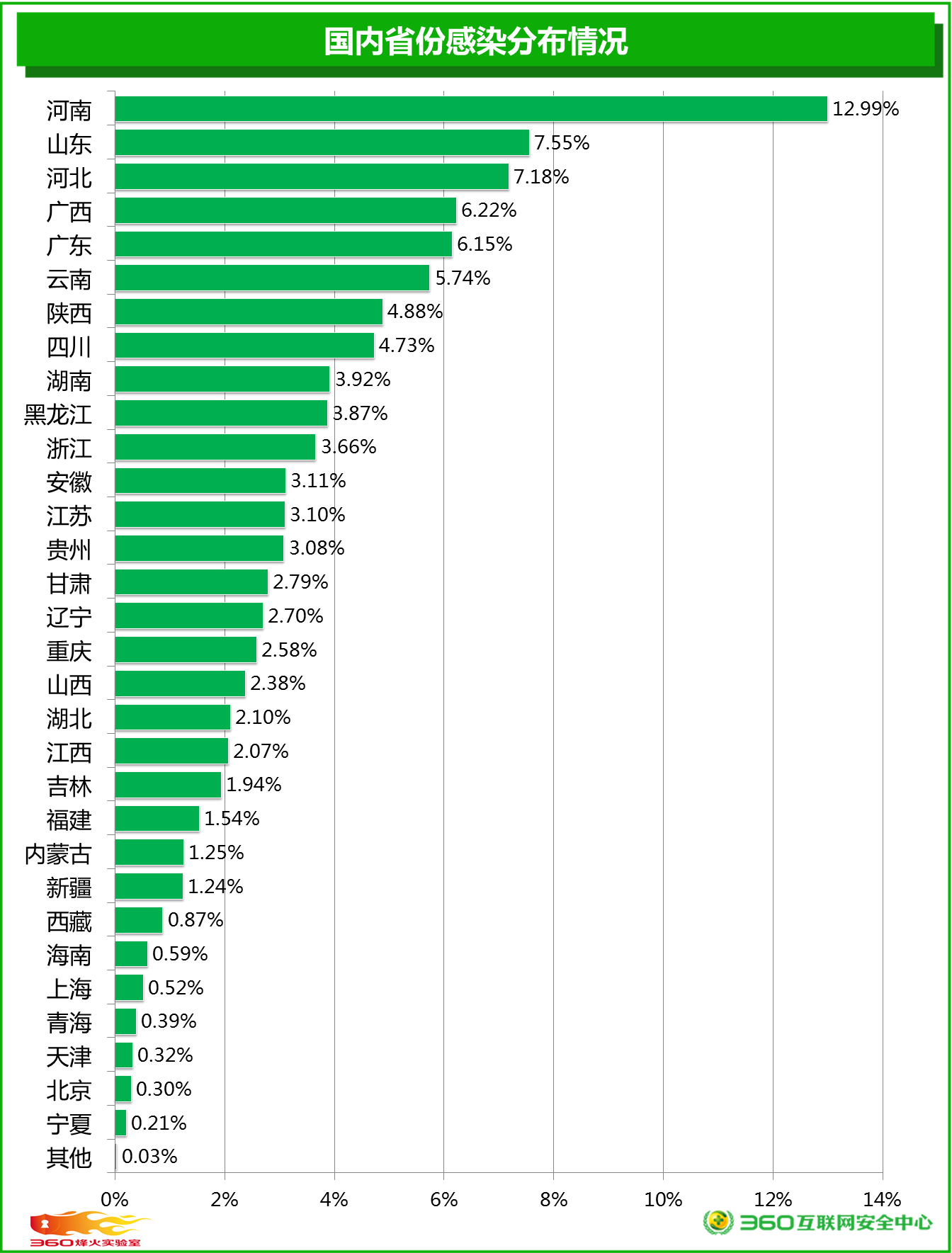


图5.2国内省份感染分布情况

从感染城市看，重点感染地区避开了国内常规的一、二线中心城市，而主要集中在中小城市。例如渭南、娄底、邯郸、菏泽等地是此次事件的重灾区。



图5.3中心和中小城市感染分布占比

从感染的手机品牌看，集中在小众品牌机型，涉及不同品牌超过150余个，我们发现主流手机品牌基本不受影响。

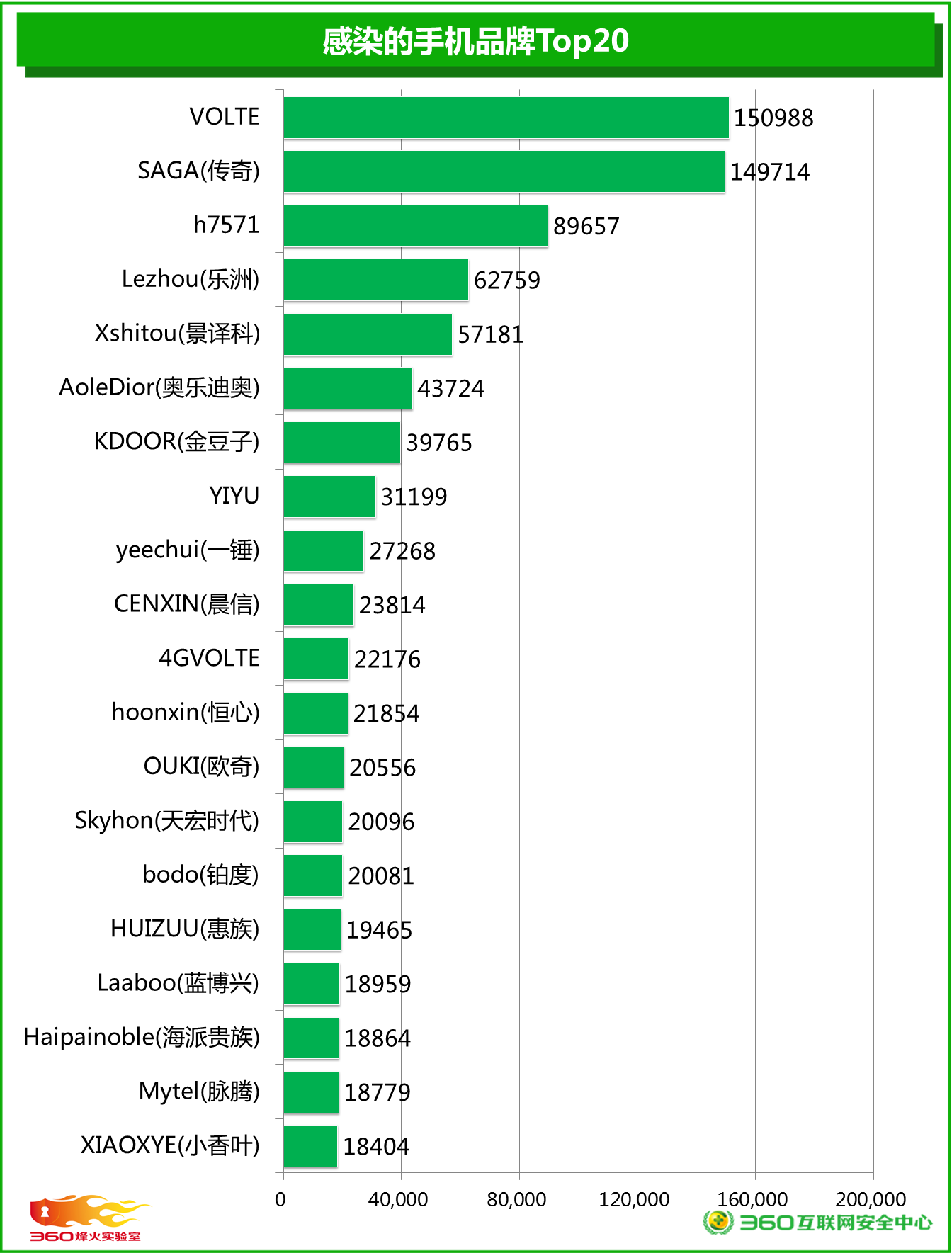


图5.4感染的手机品牌Top20

## 多家公司参与成为幕后推手

StealthBot刷量木马的庞大的刷量业务范围、与众不同的攻击目标以及迅猛爆发的态势，引起了我们高度的关注。对于其幕后的推手也做了进一步的溯源追踪分析。

分析发现，参与StealthBot制作、传播过程共涉及4家公司，其中北京市鸿途信达科技有限公司（下文简称鸿途信达）和北京盈创嘉鑫科技有限公司（下文简称盈创嘉鑫）参与制作；杭州传信网络科技有限公司（下文简称传信科技）和深圳鼎智通讯股份有限公司（下文简称鼎智通讯）参与传播。

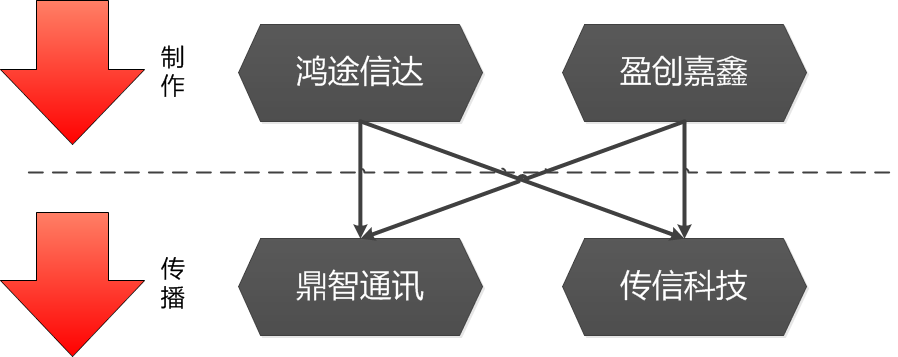


图6.1多家公司制作和传播关系

在对刷量作弊的流量监测中发现，StealthBot使用的恶意C&C域名归属于鸿途信达和盈创嘉鑫两家公司，并且使用了两家特有的渠道标识。另外还发现StealthBot样本证书名称包含了“htxd”，与鸿途信达首字母拼音缩写相同。

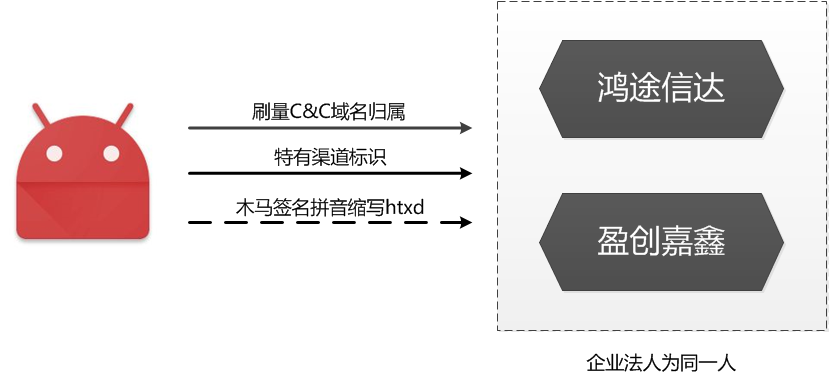


图6.2制作StealthBot直接和间接证据指向

通过网上公开信息我们发现，制作者鸿途信达和盈创嘉鑫两家公司属于科技推广和应用服务业且法定代表人均为同一个人。

StealthBot的多个推广链接归属于鼎智通讯和传信科技，通过进一步分析，我们发现两家公司的推广渠道并不相同，分别采用了手机预置和内嵌产品推广的方式。



表2

鼎智通讯是广东省一家生产移动终端为主的集团企业，总部位于深圳市南山区，涉及智能设备全过程方案开发业务，旗下生产众多小众品牌手机。

我们发现与这家公司相关的推广链接包含有usystemapks、app-release等与系统、研发、打包有关的英文词语。我们监测到的数据显示，StealthBot在2018年1月最先出现在鼎智通讯旗下的手机品牌COMIO上

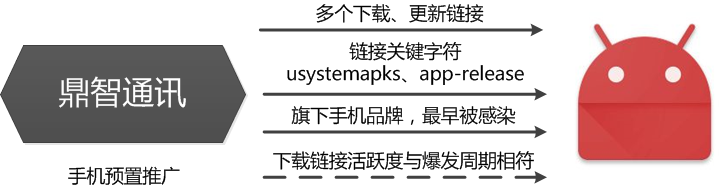


图6.3 鼎智通讯手机预置推广StealthBot直接和间接证据指向

一般情况下手机预置的恶意软件，要到达用户手里以后才开始变得活跃，所以手机预置的起始时间要稍早于恶意样本爆发时的时间。监测数据显示2017年11月前后，对应的鼎智通讯的某一子域名\*\*\*\*\*\*\*\*\*.topwisesz.com开始了异常的激增访问，这个时间正好早于StealthBot爆发大规模感染，进一步验证了我们的结论。

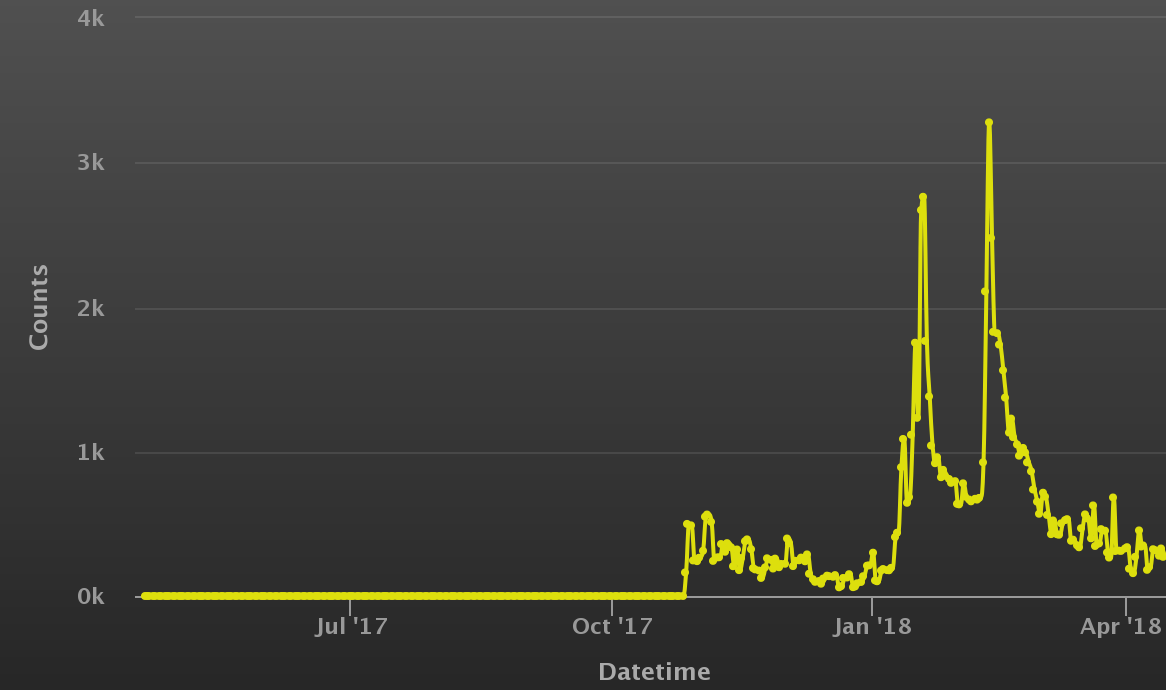


图6.4 鼎智通讯的某一子域名活跃情况（数据来源360 netlab）

另外一家公司传信科技，主要从事互联网产品运营及移动互联网产品研发，该公司主要从事"换机精灵"产品的自主研发。

我们监测到，传信科技利用自身研发的产品如“换机精灵”、“头条速览”等进行StealthBot推广传播。

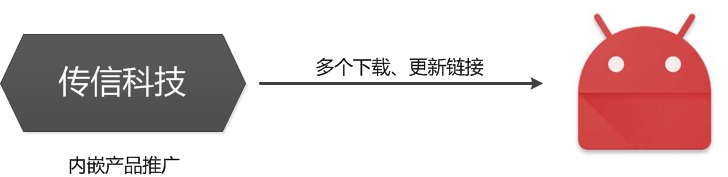


图6.5传信科技内嵌产品推广StealthBot证据指向

我们在分析流量时，发现有联网请求下载刷量木马StealthBot，StealthBot从传信科技服务器下载。



图6.6 StealthBot从传信科技服务器请求的流量数据

在一份广东省质量技术监督局2018年1月份公布的《2017年广东省手机产品质量“双随机”专项监督抽查结果公告》不合格名单列表中，我们发现了StealthBot感染的一些品牌出现在上面，证明这些有问题的小众品牌手机存在问题由来已久。

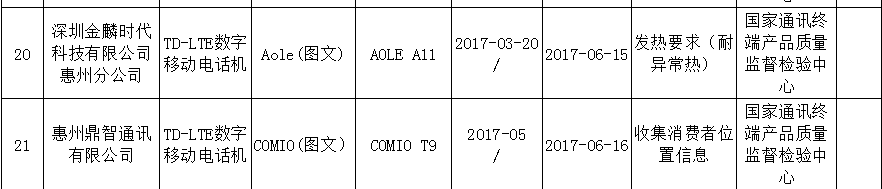


表3

小众品牌手机价格低廉，手机厂商采用多种手段收集用户隐私信息，甚至预置恶意软件，来弥补自己小众手机品牌市场份额，增加自己的收益。

3月份曝光的RottenSys恶意软件，主要是通过一家电话分销平台来进行传播的，攻击者在该环节上通过“刷机”或APP（再root）的方式，在手机到达用户手中前，在目标上安装部分RottenSys恶意软件，从而达到感染传播的效果。类似的供应链攻击在移动平台上已经屡见不鲜，供应链上的各个环节都有可能影响到最终产品和使用场景的安全性。

此次事件影响的目标机型集中在众多中小品牌手机，具有很强的针对性；同时倾销地也指向三四线中小城市，具有很强的隐蔽性难以被发现。移动生态环节面临的诸多安全威胁，也许StealthBot只是供应链分发环节中的冰山一角，我们将会持续关注。