



2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

聚力·赋能

2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

威胁情报在网络犯罪侦查中的落地应用



山东警察学院|网络空间安全与执法协同创新中心

张璇

Tel:18615177326



网络犯罪之现状



犯罪对象

非法侵入计算机信息系统
非法控制计算机信息系统
非法获取计算机信息系统数据
破坏计算机信息系统

诈骗
盗窃
淫秽色情
赌博
恐怖主义
侵犯公民个人信息
提供侵入、非法控制计算机
信息系统程序、工具
帮助信息网络犯罪活动
非法利用信息网络

犯罪工具



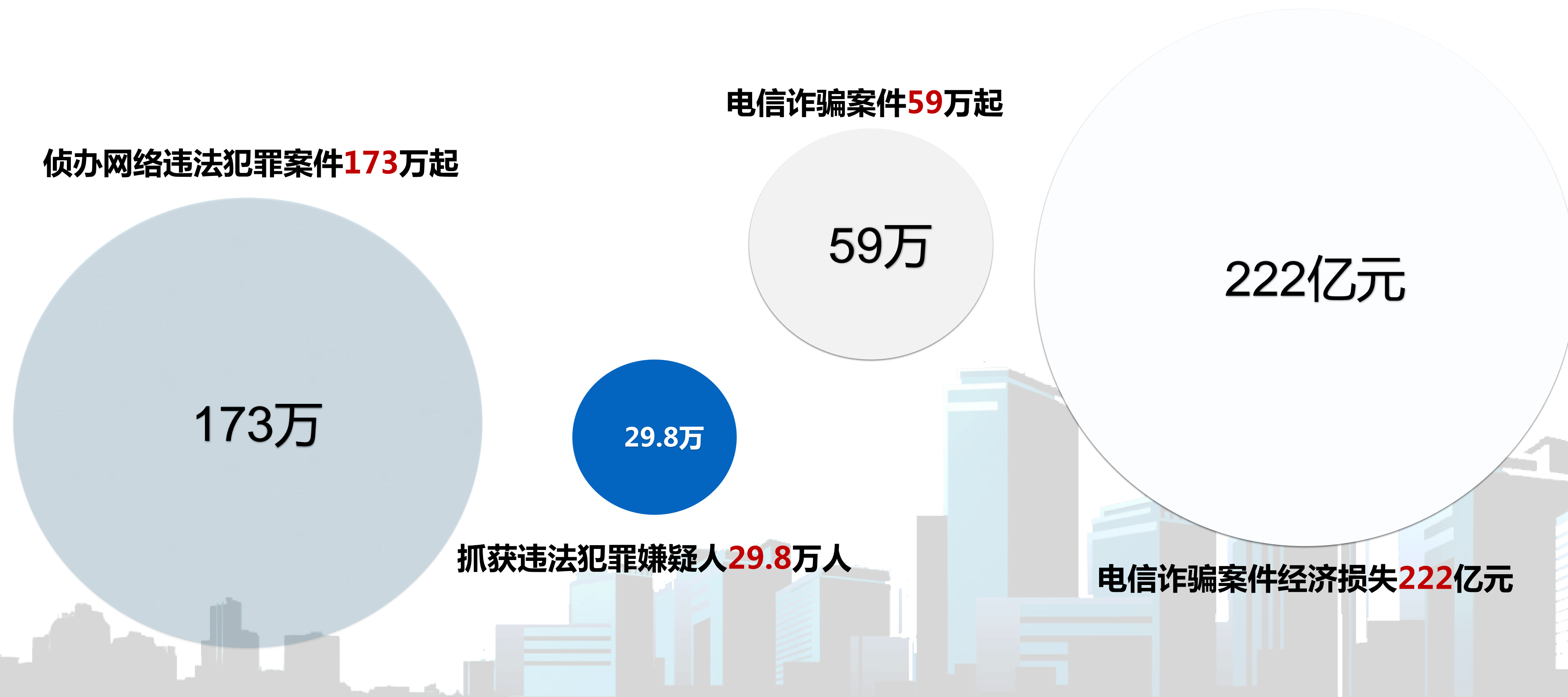
犯罪空间

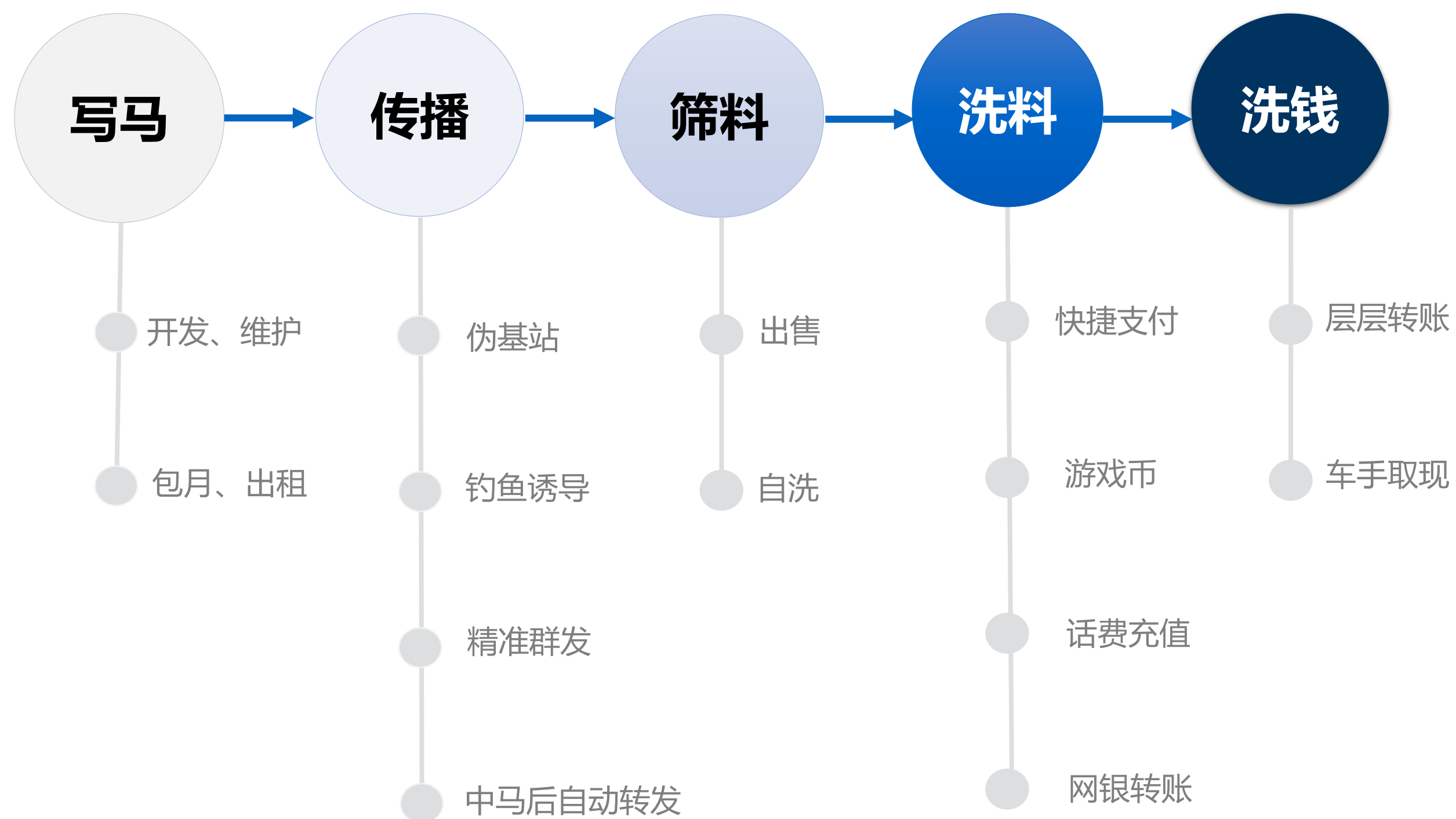
侮辱诽谤
寻衅滋事

网络犯罪是针对和利用网络进行的犯罪



2015年





黑产从业人员已经超过150万

黑产市场规模已经达到千亿



- **产业链化，分工日趋细化**
- **侵财型案件多发**
- **涉及面广，跨地域甚至跨国界犯罪现象明显**
- **发案势头猛**
- **犯罪团伙地域特征明显**
- **成本低，收益巨大**
- **移动端成为网络犯罪的重要工具和阵地**



统计难 立案难
预防难 取证难
适用法律难 认定犯罪数额难



● 网络犯罪的“打早打小”

预备行为独立入罪

针对为实施诈骗、销售违禁品、管制物品等违法犯罪活动而设立网站、通讯群组、发布信息的行为独立入罪【**非法利用信息网络罪**】

● 网络犯罪的“分工细化”

帮助行为独立入罪

针对明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助的行为独立入罪【**帮助信息网络犯罪活动罪**】



威胁情报与网络犯罪侦查

威胁情报与网络犯罪侦查



网络犯罪立体情报体系





Cartner威胁情报定义

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

一种基于证据的知识，包括了情境、机制、指标、隐含和实际可行的建议。威胁情报描述了**现存的**、或者是**即将出现**针对资产的威胁或危险，并可以用于通知主体针对相关威胁或危险采取某种响应。

情报主导安全

指挥 打击 控制 防范

情报主导警务



定义

Cartner/SANS

标准

STIX/TAXII/Cybox/NIST

平台

天际友盟/微步/360/nosec/X-Force

联盟

烽火台/乌云/阿里/通付盾/小米



美国联邦政府标准NIST 800-150 Draft

典型共享信息内容：

- IP addresses and domain names
- URLs involved with attacks
- Simple Mail Transport Protocol (SMTP) headers, email addresses, subject lines, and contents of emails used in phishing attacks
- Malware samples and artifacts
- Adversary Tactics, Techniques, and Procedures (and effectiveness)
- Response and mitigation strategies
- Exploit code
- Intrusion signatures or patterns
- Packet captures of attack traffic
- NetFlow data
- Malware analysis reports
- Campaign/actor analyses
- Disk and memory images



场景

威胁分析

网络犯罪的判断、分析调查、保留记录

威胁特征分类

网络犯罪的特征分类

威胁及安全事件应急处理

网络犯罪的处置、溯源、取证

威胁情报分享

网络犯罪情报共享、防范、预警

(STIX)



威胁情报落地应用

威胁情报落地应用



| 平台 | 主要功能 | 支持查询项 | API | 关联拓扑 |
|----|---|-------------------------|-----|------|
| 1 | 基础信息 子域名信息 实时解析 关联样本 威胁检测 历史解析 Whois 记录 | 域名、IP、MD5 | 不提供 | 无 |
| 2 | 威胁情报 子域名 可视分析 IP分析 Whois | 域名、IP、MD5 | 提供 | 有 |
| 3 | 资产管理 数据查询 威胁情报 辅助工具 | 域名、URL、备案、漏洞、泄露信息... | 提供 | 无 |
| 4 | whois记录 可疑IP 威胁报告 样本hash Email | 域名、URL、IP、MD5、Email、字符串 | 提供 | 有 |

数据量
准确率
时效性
可视化效果
...



案例一：

2016年4月30日,受害人(手机号**135567******)称收到自己熟人(**139743******)发来的短信,点击链接,自动下载名为3.apk的文件,安装后,受害人招商银行(**6225*******)账户发生网银转账6000元。

样本一：

文件: 相册3.apk
大小: 1836569 字节
修改时间: 2016年5月2日, 12:09:51
MD5: f2b0590b558a08514e1c497d400d08ba
SHA1: E84C48434A1715A7D3AABC77DFC014F9718C9259
CRC32: 3BBA687A

样本二：

文件: 相册3.apk
大小: 1837637 字节
修改时间: 2016年4月29日, 9:43:00
MD5: f4b3c7ab83402ec87a905cf6c9444074
SHA1: DD9CF591E4177B90BF05FCE26A201231F061D7B7
CRC32: A5EA2581

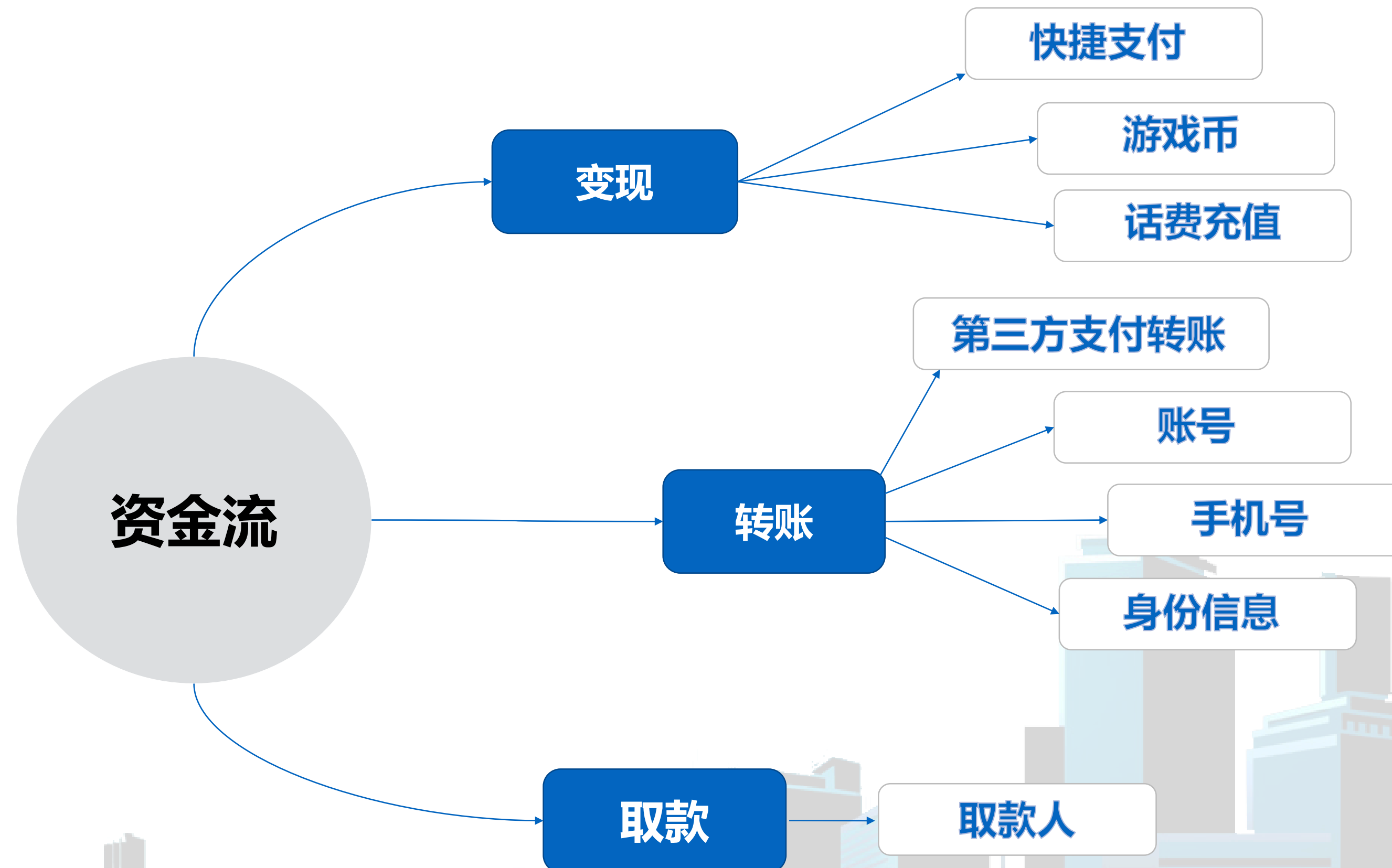
样本三：

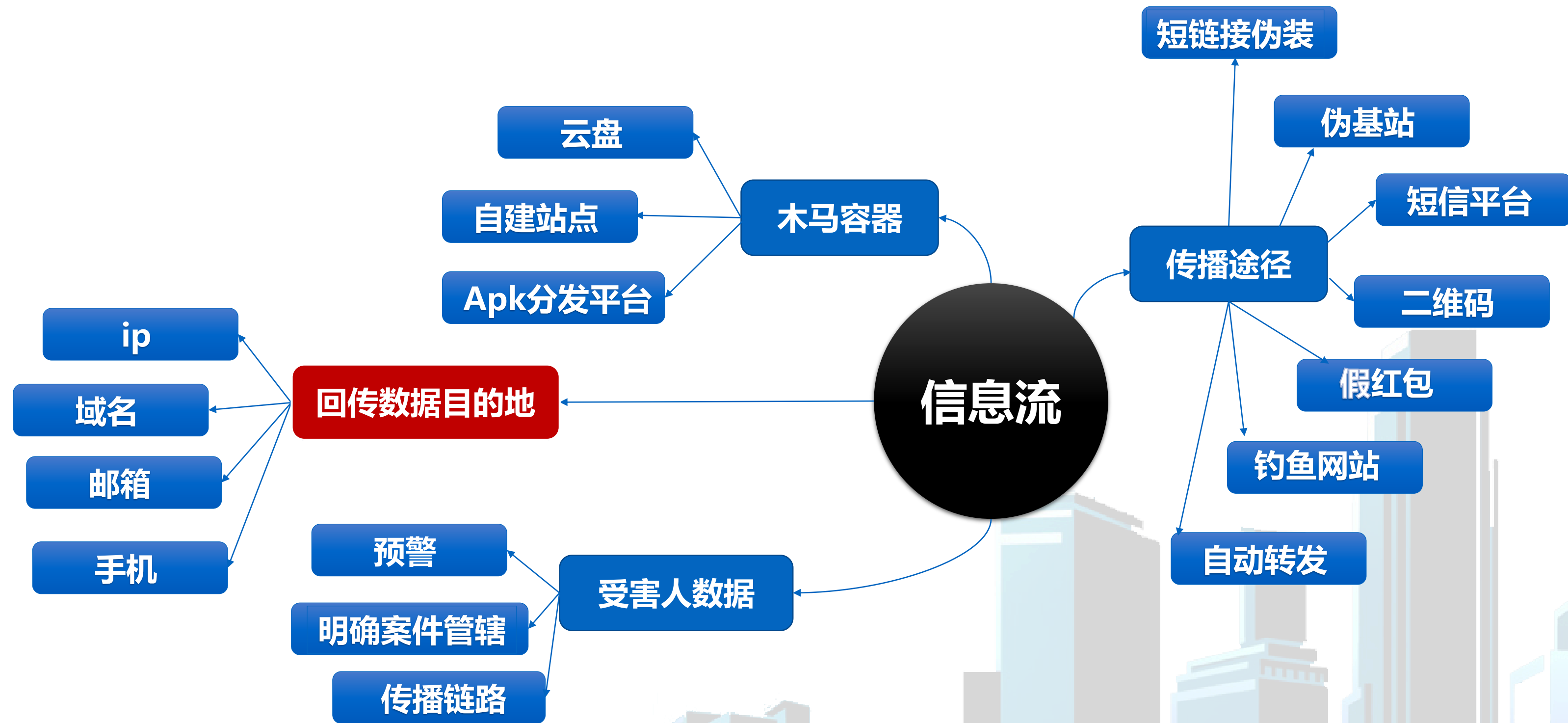
文件: 相册3.apk
大小: 1837600 字节
修改时间: 2016年4月30日, 23:01:34
MD5: 3adc9adc32eb6e5abd6b5a1ea00070ef
SHA1: C4A72CFAC7DF4CED58DDC6C627ADC72FAD694859
CRC32: 76AAA825



| 发件人 | 主题 | 日期 | 大小 |
|-------|------------------------------|--------|-------|
| shabi | 安装IMEI-860138031537621机型: DX | 下午1:54 | 6 KB |
| shabi | 安装IMEI-863777025170696机型 | 下午1:54 | 16 KB |
| shabi | 安装IMEI-863777025170696机型: DX | 下午1:54 | 88 KB |
| shabi | 安装IMEI-861166023082669机型 | 下午1:52 | 27 KB |
| shabi | 安装IMEI-A000002CB7EB37机型 | 下午1:52 | 65 KB |
| shabi | 安装IMEI-866808028945201机型: DX | 下午1:52 | 99 KB |
| shabi | 安装IMEI-866723017988627机型 | 下午1:50 | 5 KB |
| shabi | 安装IMEI-866723017988627机型: DX | 下午1:50 | 5 KB |
| shabi | 安装IMEI-359830053792971机型 | 下午1:49 | 5 KB |
| shabi | 安装IMEI-359830053792971机型: DX | 下午1:49 | 29 KB |
| shabi | 安装IMEI-861054033467296机型 | 下午1:49 | 22 KB |
| shabi | 安装IMEI-861054033467296机型: DX | 下午1:49 | 15 KB |
| shabi | 安装IMEI-359090053221048机型 | 下午1:49 | 14 KB |
| shabi | 安装IMEI-868186021004567机型 | 下午1:49 | 8 KB |
| shabi | 安装IMEI-866824023958081机型 | 下午1:49 | 4 KB |
| shabi | 安装IMEI-359090053221048机型: DX | 下午1:49 | 8 KB |
| shabi | 安装IMEI-868186021004567机型: DX | 下午1:49 | 4 KB |
| shabi | 安装IMEI-860832033130282机型 | 下午1:49 | 5 KB |
| shabi | 安装IMEI-860832033130282机型: DX | 下午1:48 | 27 KB |
| shabi | 安装IMEI-869169022717410机型 | 下午1:48 | 17 KB |
| shabi | 安装IMEI-868510025686246机型: DX | 下午1:48 | 38 KB |
| shabi | 安装IMEI-869803026898509机型: DX | 下午1:48 | 38 KB |
| shabi | 安装IMEI-866930020041886机型 | 下午1:48 | 5 KB |
| shabi | 安装IMEI-866930020041886机型: DX | 下午1:48 | 27 KB |
| shabi | 安装IMEI-867051022108836机型: DX | 下午1:47 | 12 KB |
| shabi | 安装IMEI-860443035436600机型 | 下午1:47 | 11 KB |
| shabi | 安装IMEI-860443035436600机型: DX | 下午1:47 | 94 KB |
| shabi | 安装IMEI-A100004201AC19机型 | 下午1:46 | 4 KB |
| shabi | 安装IMEI-867051022108836机型 | 下午1:46 | 11 KB |
| shabi | 安装IMEI-A100004201AC19机型: DX | 下午1:46 | 12 KB |
| shabi | 安装IMEI-869037024470819机型 | 下午1:44 | 4 KB |
| shabi | 安装IMEI-865877021903880机型 | 下午1:44 | 3 KB |
| shabi | 安装IMEI-865877021903880机型: DX | 下午1:43 | 49 KB |
| shabi | 安装IMEI-A0000055EF0E5D机型 | 下午1:43 | 19 KB |

Sha*@tencent.com**
qq520520







该恶意代码直接关联的域名有：

lcnover.com(恶意代码存放空间)

tenceny.com(恶意代码上传用户隐私到网易企业免费邮箱shabi@tenceny.com，可以注册自己设定的后缀，对应已注册的域名)

| | |
|---------|-----------------------|
| 注册域名 | lcnover.com |
| 创建时间 | 2016-04-12 15:49:04 |
| 域名过期时间 | 2017-04-12 15:49:04 |
| 注册人 | wanmengshao |
| 域名管理员邮箱 | 32425545@qq.com |
| 注册管理员电话 | +86.0,+86.03216273623 |

| 域名 | 注册人 | 邮箱 | 注册日 | 到期日 |
|--------------------|-------------|-----------------|------------|------------|
| lcnover.com | wanmengshao | 32425545@qq.com | 2016-04-12 | 2017-04-12 |
| xuexiaotongzhi.com | wanmengshao | 32425545@qq.com | 2016-02-20 | 2017-02-20 |

| 解析次数 | 解析结果 | 域名 | 首次解析时间 | 最后解析时间 |
|------|--------------|-------------|---------------------|---------------------|
| 8031 | 45.64.112.28 | lcnover.com | 2016/04/18 00:00:00 | 2016/05/03 00:00:00 |



该恶意代码直接关联的域名有：

lcnover.com 同IP解析历史45.64.112.28

| 解析结果 | 解析时间 | 注册邮箱 | 注册人 |
|-----------------|------------------|-------------------------|-------------|
| www.lcnover.com | 2016/5/3 14:58 | 32425545@qq.com | wanmengshao |
| lcnover.com | 2016/5/3 14:44 | 32425545@qq.com | wanmengshao |
| wap.lcnover.com | 2016/4/29 15:29 | 32425545@qq.com | wanmengshao |
| www.ssc1880.com | 2015/11/1 10:54 | 406229685@qq.com | li dong |
| ssc1880.com | 2015/10/7 21:52 | 406229685@qq.com | li dong |
| d.711xy.com | 2015/7/22 20:54 | privacy@sun-privacy.com | |
| m.ssc1880.com | 2015/4/7 23:15 | 406229685@qq.com | li dong |
| 6h.ssc1880.com | 2015/3/22 14:20 | 406229685@qq.com | li dong |
| www.nnn7777.com | 2015/1/7 10:06 | sdds5@163.com | sds sd |
| www.xunyou7.com | 2014/12/19 13:20 | 755188400@qq.com | lirong shi |
| www.nnn3333.com | 2014/12/19 11:32 | sdds5@163.com | sds sd |
| www.ttt4444.com | 2014/12/17 13:16 | sdds5@163.com | sds sd |
| www.nnn1111.com | 2014/12/16 10:51 | sdds5@163.com | sds sd |
| xunyou7.com | 2014/12/15 21:12 | 755188400@qq.com | lirong shi |
| nnn7777.com | 2014/12/14 17:40 | sdds5@163.com | sds sd |
| www.qqq4444.com | 2014/12/12 19:28 | sdds5@163.com | sds sd |
| nnn1111.com | 2014/12/6 6:34 | sdds5@163.com | sds sd |
| nnn3333.com | 2014/12/6 6:34 | sdds5@163.com | sds sd |
| ttt4444.com | 2014/12/6 6:34 | dfgkfdj8899@126.com | lirong shi |
| qqq4444.com | 2014/12/6 6:33 | sdds5@163.com | sds sd |
| www.vvv4444.com | 2014/12/6 6:33 | dfgkfdj8899@126.com | lirong shi |
| vvv4444.com | 2014/12/6 6:33 | dfgkfdj8899@126.com | lirong shi |





同IP解析历史

ssc1880.com

xunyou7.com

vvv4444.com

nnn7777.com

nnn1111.com

nnn3333.com

ttt4444.com

qqq4444.com

注册人: Wanmengshao

406229685@qq.com

li dong

406229685

755188400@qq.com; dfgkfdj8899@126.com

lirong shi

www.nxnmgsh.com 澳门'官方网站,网络'网,澳门'公司
2016年2月7日 - 访问网址: http://www.nxnmgsh.com 关键词: 澳门'官方网站,网络'网,澳门'公司
..Tech Email: dfgkfdj8899@126.com Name Server: F1G1NS1.DNSPOD.NET Nam...
www.70dir.com/seo/repo... - 百度快照 - 60%好评

75518840

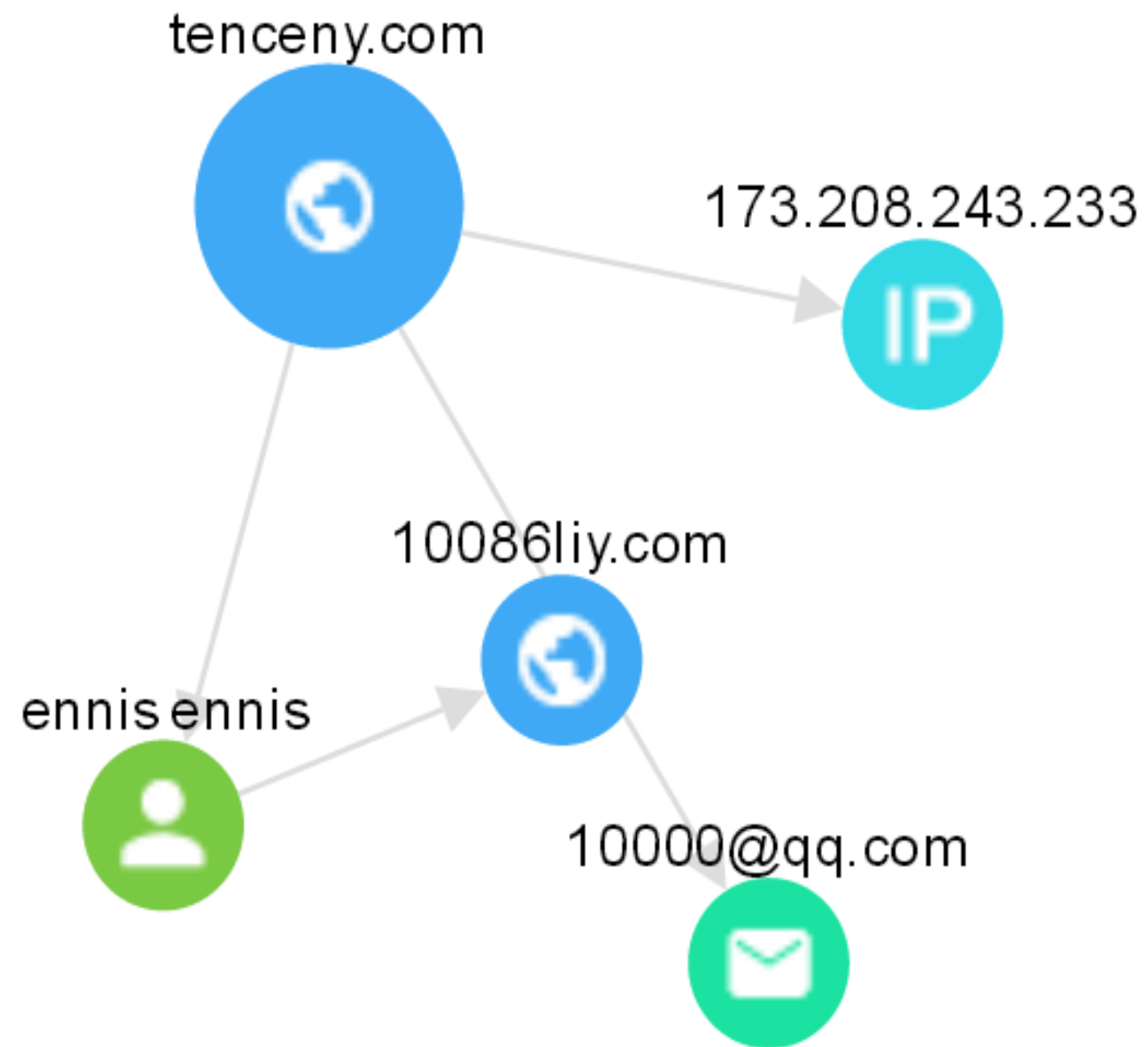
sdds5@163.com

sds sd

梳理结果：
QQ:32425545\406229685\755188400 (经搜索标示位于广西、买卖备案域名等相关)
邮箱：sdds5@163.com、dfgkfdj8899@126.com后者与赌博网站关。



tenceny.com



| 解析次数 | 解析结果 | 域名 | 首次解析时间 | 最后解析时间 |
|------|-------------------|-------------|---------------------|---------------------|
| 2 | 173.208.243.233 | tenceny.com | 2015/04/04 00:00:00 | 2015/04/04 00:00:00 |
| 1 | 123.125.81.12 | tenceny.com | 2014/08/18 00:00:00 | 2014/08/18 00:00:00 |
| 19 | ns11.xincache.com | tenceny.com | 2014/12/10 00:00:00 | 2014/12/10 00:00:00 |

| 注册域名 | tenceny.com |
|---------|---------------------|
| 创建时间 | 2014-12-09 13:33:51 |
| 域名过期时间 | 2015-12-09 13:33:51 |
| 注册人 | ennis ennis |
| 域名管理员邮箱 | 10000@qq.com |
| 注册管理员电话 | +86.1000 10086100 |



tencent.com

网易 免费企业邮
ym.163.com

shabi@tencent.com [邮箱首页, 退出]

收信 写信

联系人分组 [新建组]

其他(0)

| 写信 | 打印 | 名称 | 邮箱地址 |
|--------------------------|----|---------|----------------------|
| <input type="checkbox"/> | | 天下第一 | 10000@tencent.com |
| <input type="checkbox"/> | | 2016发发 | 2016fafa@tencent.com |
| <input type="checkbox"/> | | 官方邮件 | call110@tencent.com |
| <input type="checkbox"/> | | dashabi | dashabi@tencent.com |
| <input type="checkbox"/> | | 恶魔猎手 | emls@tencent.com |
| <input type="checkbox"/> | | facai | facai@tencent.com |
| <input type="checkbox"/> | | 菊花 | juhua@tencent.com |
| <input type="checkbox"/> | | miss | miss@tencent.com |
| <input type="checkbox"/> | | 请帖 | qintie@tencent.com |
| <input type="checkbox"/> | | tencent | qq@tencent.com |
| <input type="checkbox"/> | | 超级会员项目组 | server.@tencent.com |
| <input type="checkbox"/> | | 腾讯 | service@tencent.com |
| <input type="checkbox"/> | | shabi | shabi@tencent.com |
| <input type="checkbox"/> | | 超级会员项目组 | svip@tencent.com |
| <input type="checkbox"/> | | 腾讯中心 | tencent@tencent.com |
| <input type="checkbox"/> | | 天天向上 | ttxs@tencent.com |
| <input type="checkbox"/> | | 王宝 | wangbao@tencent.com |
| <input type="checkbox"/> | | 发财 | wocao@tencent.com |
| <input type="checkbox"/> | | 香烟 | xiangyan@tencent.com |
| <input type="checkbox"/> | | 域名服务 | yuming@tencent.com |

写信 打印

关联分析以人工查询分析为主
数据的来源比较单一





案例二：





案例二：

平台一

gdfuyi.cn

实时解析

| 区域类别 | 记录 | 过期时间(s) |
|------|----------------|---------|
| IN | 43.255.106.225 | 7200 |

whois 记录

| | | | |
|----------------------|--|---------|------------------|
| 注册域名 | gdfuyi.cn | 注册人 | 惠阳区新圩富艺丝花厂 |
| 域名哈希值 | e90679ee5ee6d1a721d25bd2a13cd34a | 域名管理员邮箱 | cndomain@300.cn |
| 域名状态 | ["ok"] | 注册管理员电话 | |
| 创建时间 | 2009-01-13 15:50:58 | 注册管理员传真 | |
| 域名过期时间 | 2015-01-13 15:50:58 | 注册人所属组织 | |
| 最后更新时间 | | 国家代码 | |
| DNS 请求报文头 | [Querying whois.cnnic.cn] [whois.cnnic.cn] | 注册人所在省份 | |
| 注册域名 | 中企动力科技股份有限公司 | 注册人所在城市 | |
| 域名服务器 | ["ns2.ce.net.cn","ns1.ce.net.cn"] | 注册人地址 | |
| Identity | 2a50902ab69e3f942454af09c1c1d408 | 邮编 | |
| Whois Server | | 域名ID | 1007141424152990 |
| 查看详情 | | 记录时间 | |

关联样本



案例二：

平台二

威胁情报 IP分析 子域名 Whois **可视分析**

基础数据信息

- 🌐 域名
- 📄 样本
- 🌐 IP
- ✉️ whois注册邮箱
- 👤 whois注册名

威胁情报数据

- 🌐 域名
- 📄 文件HASH
- 🌐 URL
- 🌐 IP
- ⋮ 其它

提示

- 分类数据最大显示结点数：50
- 点击图标，查看详细内容并访问链接

威胁情报 IP分析 子域名 **Whois** 可视分析

当前注册信息

| | |
|-------|------------------------------------|
| 注册者 | 张光信 (相关域名 499 个) |
| 注册机构 | |
| 邮箱 | 2284683387@qq.com (通用注册邮箱不再显示相关域名) |
| 地址 | |
| 电话 | |
| 注册时间 | 2016-05-01 00:00:00 |
| 过期时间 | 2017-05-01 00:00:00 |
| 更新时间 | |
| 域名服务商 | 厦门市中资源网络服务有限公司 |
| 域名服务器 | ns1.cnolnic.com; ns2.cnolnic.com |

历史注册信息

| | |
|------------|--|
| 日期 | 重要信息更新 |
| 2016-05-03 | 修改： 注册者: 崔向阳 → 张光信 邮箱: cuijiahaocxy@163.com → 2284683387@qq.com |
| 2016-04-22 | 非重要更新, 可点击左侧日期查看全部信息 |
| 2016-03-25 | 非重要更新, 可点击左侧日期查看全部信息 |
| 2016-03-09 | 非重要更新, 可点击左侧日期查看全部信息 |



案例二：

管理首页 > ICP备案查询

平台三

ICP备案查询

gdfuyi.cn 搜索

共发现 1 条纪录，当前账户显示 10 条，需要更多请[升级账号](#)，可通过[API](#)获取全部结果。

| 域名 | 编号 | 单位名称 |
|-----------|----------------------------------|------------|
| gdfuyi.cn | 粤ICP备09008417号-1(粤ICP备09008417号) | 惠阳区新圩富艺丝花厂 |



案例二：

查询结果

gdfuyi.cn



cuijiahaocxy@163.com

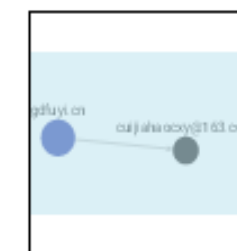


域名：gdfuyi.cn

注册信息

Domain Name: gdfuyi.cn
ROID: 20150308s10001s74196570-cn
Domain Status: ok
Registrant ID: 1556-652374-d-01
Registrant: 崔向阳
Registrant Contact Email: cuijiahaocxy@163.com
Sponsoring Registrar: 成都西维数码科技有限公司
Name Server: f1g1ns1.dnspod.net
Name Server: f1g1ns2.dnspod.net
Registration Time: 2015-03-08 21:36:12
Expiration Time: 2016-03-08 21:36:12
DNSSEC: unsigned

平台四



数据的时效性、准确性问题

北京天际友盟信息技术有限公司版权所有

Copyright © TianJi Partners Website 2



案例三：



▶ **第一步：骗子冒充民警谎称涉嫌洗钱案**

▶ **第二步：发送链接，“账户自清”**

刘女士电话被转到“上海市嘉靖公安局刑侦大队”的“李警官”手上，“李警官”让刘女士去酒店开个房间，方便调查。刘女士开房后，接到对方使用+9902159980197的来电，称她已经被通缉，并向她的手机号码发送链接<http://400800110.co/h/apk/fl.apk>。刘女士点击链接，手机下载安装一款名为“公安部案件查询系统”的app。

▶ **第三步：填写个人信息，钱款丢失**



案例三：

平台一

205 414

| 类型 | 解析结果 | 域名 | 首次解析时间 | 最后解析时间 |
|----|---------------|--------------|---------------------|---------------------|
| A | 142.4.126.185 | 400800110.co | 2015/08/11 00:00:00 | 2015/12/24 00:00:00 |
| A | 142.4.112.49 | 400800110.co | 2016/05/12 00:00:00 | 2016/07/05 00:00:00 |

首页 上一页 1 下一页 末页

| 记录 | 过期时间(s) | 类型 |
|--------------|---------|----|
| 142.4.112.49 | 600 | A |

首页 上一页 1 下一页 末页

400800110.co

注册人

registration private

域名管理员邮箱

400800110.co@domainsbyproxy.com

["clientdeleteprohibited","clientrenewprohibited","clienttransferprohibited","clientupdateprohibited"]

注册管理员电话

+1.4806242598,+1.4806242599

注册管理员传真

注册人所属组织

domains by proxy, llc

2015-07-23 21:06:17

2016-07-23 07:59:59

507e-01-53 01:28:28

507e-01-53 51:08:11

domainsbyproxy.com

域名代理

注册人联系电话

注册人联系传真

domains by proxy, llc



平台二

案例三：

400800110.co 分析报告

800110.co 分析报告

域名服务商 GODADDY.COM, INC.
域名服务器 ns05.domaincontrol.com; ns06.domaincontrol.com
Alexa排名 N/A

域名服务商 GODADDY.COM, INC.
域名服务器 ns05.domaincontrol.com; ns06.domaincontrol.com
Alexa排名 N/A

威胁情报 IP分析 子域名 Whois 可视分析

威胁情报 IP分析 子域名 Whois 可视分析

IP地址

IP地址 (共有 0 个域名指向此地址)

地理位置

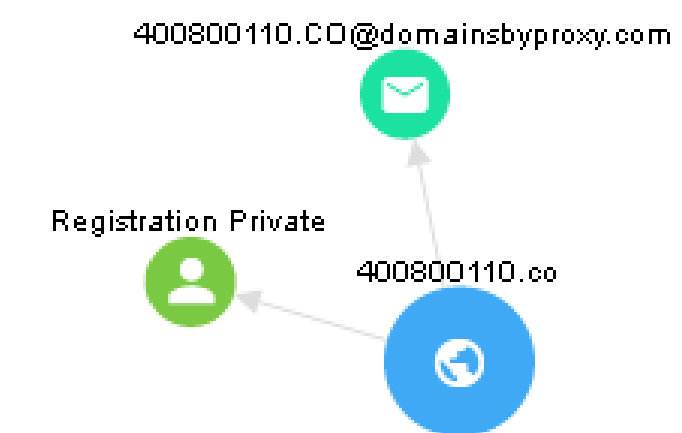
ASN 无ASN信息

历史解析记录

没有数据

指向同一IP的域名列表

没有数据





案例三：

平台三

全球网站检索 发现你不知道的

? 搜索

总计 135487438 条纪录，搜索 **domian="400800110.co"** 用时 5365毫秒，模式:normal。 当前账户显示 100条，需要更多请[升级账号](#)，可通过[API](#)获取全部结果。

| | |
|--|--|
| <p>news.msc99.co</p> <p>申博备用网站 太阳城申博 申博亚洲 www.22msc.net</p> <p> 192.229.76.118</p> <p>msc99.co</p> <p>更新时间：2015-08-05</p> <p></p> | <pre>HTTP/1.1 200 OK Connection: close Date: Wed, 05 Aug 2015 04:50:15 GMT Content-Type: text/html; charset=gb2312 Server: IIS X-Powered-By: WAF/2.0, WAF/2.0 Set-Cookie: safedog-flow-item=BD77327EB801C66CCED81C6FEF41113B; expires=Wen, 5-Aug-2015 15:59:15 GMT; domain=msc99.co; path=/</pre> |
| <p>5345.co</p> <p>新葡京娱乐城--专注网上娱乐，老牌信誉,值得信赖</p> <p> 107.167.10.91</p> <p>5345.co</p> <p>更新时间：2015-08-10</p> <p></p> | <pre>HTTP/1.1 200 OK Content-Type: text/html Content-Encoding: gzip Last-Modified: Sat, 08 Aug 2015 19:11:04 GMT Accept-Ranges: bytes Etag: "af46b8f8dd2d01:0" Vary: Accept-Encoding Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Date: Sun, 09 Aug 2015 06:07:10 GMT Content-Length: 325</pre> |
| <p>news.msc44.co</p> <p>申博娱乐城现金网网址 菲律宾太阳城直营网 申博娱乐直营网 www.98msc.net</p> <p> 192.229.76.113</p> <p>msc44.co</p> <p>更新时间：2015-08-05</p> <p></p> | <pre>HTTP/1.1 200 OK Connection: close Date: Wed, 05 Aug 2015 04:50:14 GMT Content-Type: text/html; charset=gb2312 Server: IIS X-Powered-By: WAF/2.0, WAF/2.0 Set-Cookie: safedog-flow-item=BD77327EB801C66CCED81C6FEF41113B; expires=Wen, 5-Aug-2015 15:59:14 GMT; domain=msc44.co; path=/</pre> |



案例三：

142.4.112.49

查询结果

每页显示条目: 10 检索:

| value | type |
|--------------|------|
| 142.4.112.49 | IP |

显示 1 条,共 1 条记录 页数: 上一页 1 下一页

IP : 142.4.112.49

IP注册信息

| 属性 | 信息 |
|------|---------|
| 国家 | 美国 |
| 城市 | 圣何塞 |
| 网络名称 | PT-82-4 |

AS信息

| ASN | AS名称 | AS归属 |
|---------------|------------|------------------|
| 54600 (正常) | PEGTECHINC | PEG TECH INC, US |

IP段

142.4.X.X 浏览
142.4.112.X 浏览

Whois信息的局限性

平台四



未来可期



- 从“有无”到“优劣”
- 从“独立”到“共享”
- 从“已知”到“未知”

- 立足应用场景的深度分析工具
- 可视化工具
- 评价指标



互联网+犯罪

发现难 取证难 打击难 统计难 预防难

理念 技术 协作

战役才刚刚开始.....

山东警察学院网络空间安全与执法协同创新中心



2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

**谢谢！
好客山东欢迎您！
2016.7**