白帽汇针对金融领域
伪基站钓鱼黑产的分析报告

最新版本：v1.0

最后编辑日期：2016年03月25日

北京白帽汇科技有限公司

Beijing Baimaohui Technologies Co. Ltd.

目录

概述

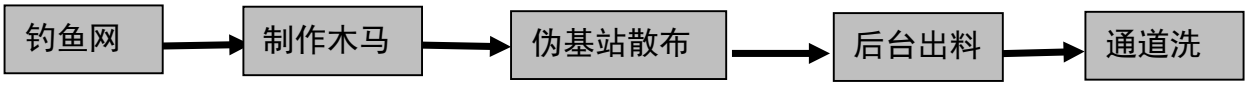
伪基站钓鱼一直以来都是导致金融巨额损失的重灾区，即使在法律和技术进行安全管控的情况下，形式也变得越来越严峻。黑产（黑色地下产业的简称）会通过严密的组织和流程获取金融用户的账号信息(银行卡账号,密码,身份证号，CVV 等），进而进行大批量金额的转出。根据《中国互联网站发展状况及其安全报告（2015）》显示，共有 6116 个境外 IP 地址承载了 93136 个针对我国境内网站的仿冒页面，仿冒页面数量较 2013 年增长 2.1 倍，虽然各部门都在配合打击钓鱼欺诈类网站，但是越来越多的黑产团伙，开始利用频繁更改域名，租用境外服务器等手段躲过有关机构的监管拦截，导致钓鱼欺诈现象屡禁不止，根据相关监控数据显示每天都有大量新增的钓鱼上线，这些钓鱼网站时效性短，部署搭建容易，成本低廉。保守估计，中国金融领域每年遭受伪基站钓鱼攻击导致的金额损失高达 100 亿。

白帽汇作为“中国互联网网络安全威胁治理联盟”的首批成员单位，在 2016 年三月份针对金融领域的伪基站钓鱼的黑色产业链进行了深入的调查分析，我们在分析攻击流程的基础上加上了**黑产反制**的技术，通过技术手段获取了钓鱼网站的后台或数据的管理权限，获取了受害用户的详细清单，钓鱼网站的源代码，拦截短信的 APK，以及伪基站发送短信的模板等信息。在本次调查过程中我们发动广泛的白帽子的力量，针对追踪收集到的 **1947** 个钓鱼网站进行反制和溯源分析，深入了解和还原出该条黑色产业链的各个渠道流程。最终，我们从钓鱼网站的后台截获了超过 **50000** 个金融客户的账号，去重后有超过 **19000 受害用户**

信息，账号主要覆盖工商银行，建设银行，农业银行，储蓄银行，中国银行，以及其他城商行。保守估计受害金额达 **2 亿**元，其中单个用户最大余额超过一百万。受骗人群主要集中在 20-30 岁的人群，地域分布在 二、三 线城市为主。伪冒的钓鱼站中又以工商银行和中国移动充值居多，而通过对受骗人群性别统计，其中女性受骗率远远高于男性。在整个产业链条中，在后台进行数据清洗（行话又称“洗料”）的人获利最多，远远高于产业链中实施伪基站钓鱼的其他环节。

伪基站钓鱼产业链分析

伪基站钓鱼黑产简单流程示意图：



各个环节工作内容：

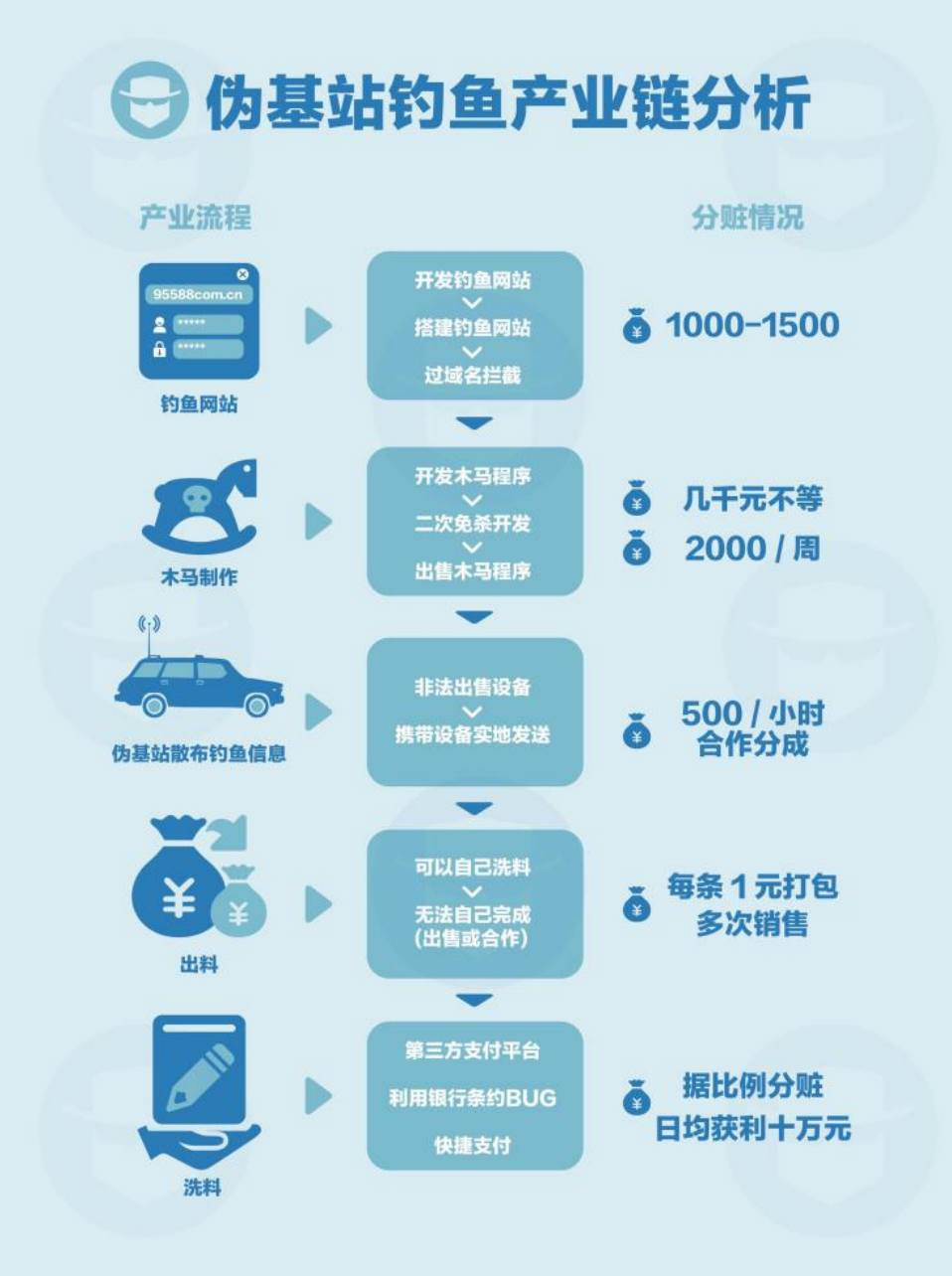
制作网站：有专人抢注类似于运营商，各大银行机构的域名进行出售或自己用，有专业的人员进行仿站模仿类似于运营商、各个银行的网站，然后购买美国或者香港免备案服务器进行搭建后制作过域名拦截程序。据了解市面上搭建一个完整的钓鱼网站价格也就在 1000 元到 1500 元左右。

木马制作：由程序开发人员进行开发后，以几千元不等的价格将源码卖给下级代理进行二次开发出售（根据各大杀毒库的更新情况制作“免杀”）以每周 2000 元进行出售。

伪基站发送钓鱼短信：这个一般为线下交易，，包吃包住包油钱以每小时 500 元左右为酬劳或以合作分成的方式,让有伪基站设备的人带着伪基站游走在繁华的街区进行大范围的撒网（发送钓鱼网站）。

“出料”：将钓鱼网站后台收到的数据进行筛选整理（利用各个银行的在线快捷支付功能情况查余额,看看是否可以直接消费进行转账或第三方支付进行消费），自己无法将余额消费的将会以余额的额度以不同的价格出售(大部分会打包起来以每条 1 元的价格进行多次叫卖）余额巨大的有时还会找人合作进行“洗料”。

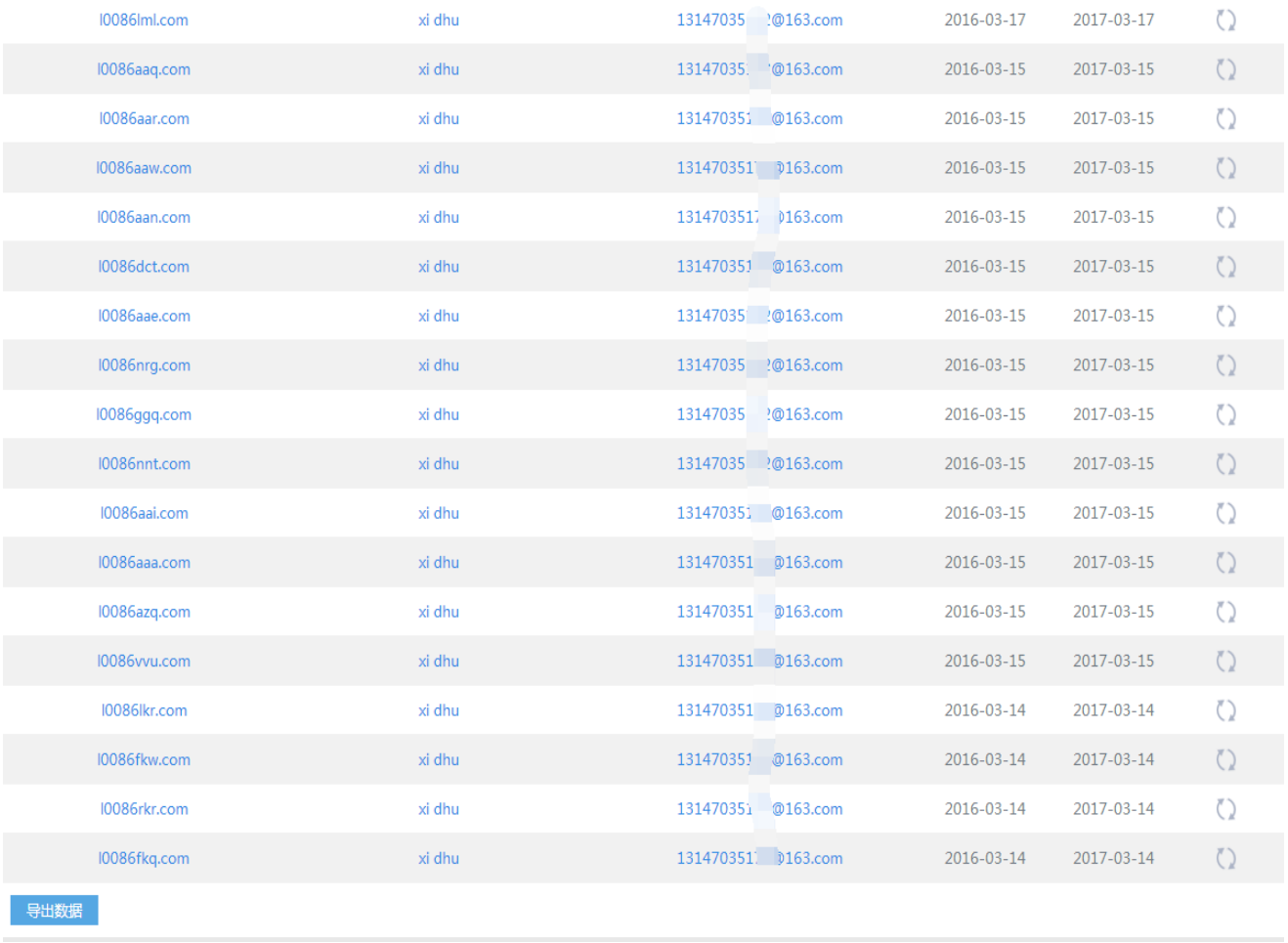
“洗料”：通过多种方式将“料”进行变现，一般开通快捷支付充值水电、话费、游戏币或者利用其他存在第三方支付转账接口和银行快捷支付漏洞等，将“四大件”变成成现金后通过各种规避追查的手段与合伙人按比例（一般以料的额度按 5：5　4：6　3：7 这些比例）进行分账，日均可以赚取 10 万元以上。



1. 虚假域名

在我们的调查中他们会事先购买大量类似于运营商、银行机构的域名。在这个完整的产业链里有一些就是出售这些域名的 ,由于安全厂商 ,以及公安的打击，

所以通常域名的存活周期也是非常的短，一般有效周期为 1-7 天，基本是打一枪换一个地方，需要使用到大量的域名。



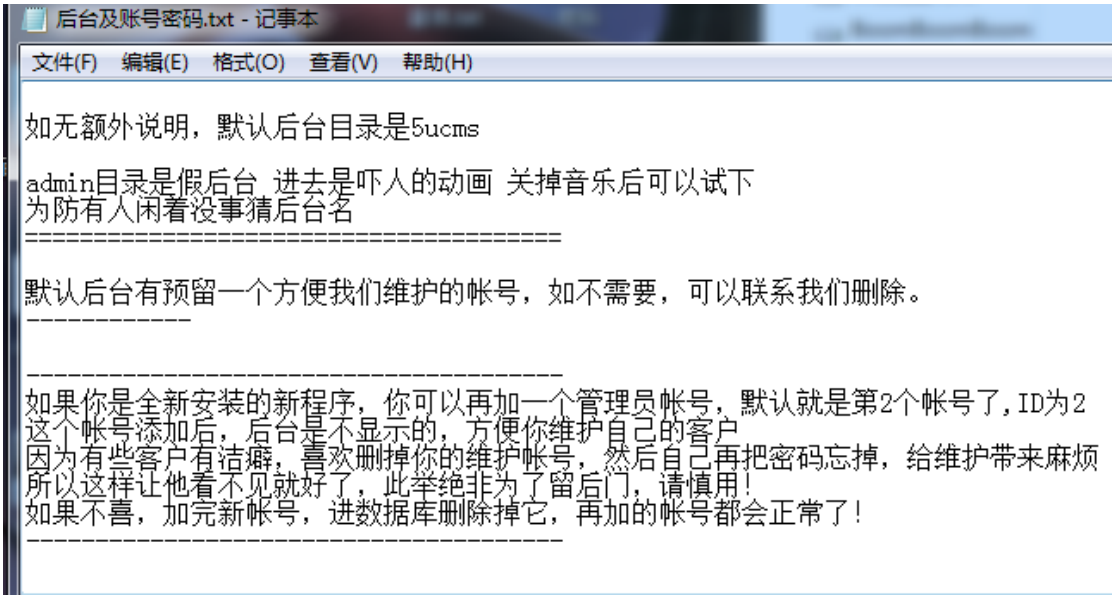
l0086lml.com	xi dhu	13147035 2@163.com	2016-03-17	2017-03-17
l0086aaq.com	xi dhu	13147035 @163.com	2016-03-15	2017-03-15
l0086aar.com	xi dhu	13147035 @163.com	2016-03-15	2017-03-15
l0086aaw.com	xi dhu	1314703517 @163.com	2016-03-15	2017-03-15
l0086aan.com	xi dhu	1314703517 @163.com	2016-03-15	2017-03-15
l0086dct.com	xi dhu	1314703517 @163.com	2016-03-15	2017-03-15
l0086aae.com	xi dhu	13147035 2@163.com	2016-03-15	2017-03-15
l0086nrg.com	xi dhu	13147035 2@163.com	2016-03-15	2017-03-15
l0086ggq.com	xi dhu	13147035 2@163.com	2016-03-15	2017-03-15
l0086nnt.com	xi dhu	13147035 2@163.com	2016-03-15	2017-03-15
l0086aai.com	xi dhu	13147035 @163.com	2016-03-15	2017-03-15
l0086aaa.com	xi dhu	13147035 @163.com	2016-03-15	2017-03-15
l0086azq.com	xi dhu	13147035 @163.com	2016-03-15	2017-03-15
l0086vvu.com	xi dhu	13147035 @163.com	2016-03-15	2017-03-15
l0086lkr.com	xi dhu	13147035 @163.com	2016-03-14	2017-03-14
l0086fkw.com	xi dhu	13147035 @163.com	2016-03-14	2017-03-14
l0086rkr.com	xi dhu	13147035 @163.com	2016-03-14	2017-03-14
l0086fkq.com	xi dhu	1314703517 @163.com	2016-03-14	2017-03-14

导出数据

2. 钓鱼网站

接来下就是制作出售维护钓鱼网站的。成本很低，固定的几套源码修改下直接就可以搭建起来。

在我们反制下的许多钓鱼站之后在源码里发现一些有趣的东西——黑吃黑，在源码的说明里面这样写着**“默认后台有预留一个方便我们维护的帐号，如不需要，可以联系我们删除。”**然后下面那段文字就是教你怎么添加一个后门帐号（“方便维护”）。

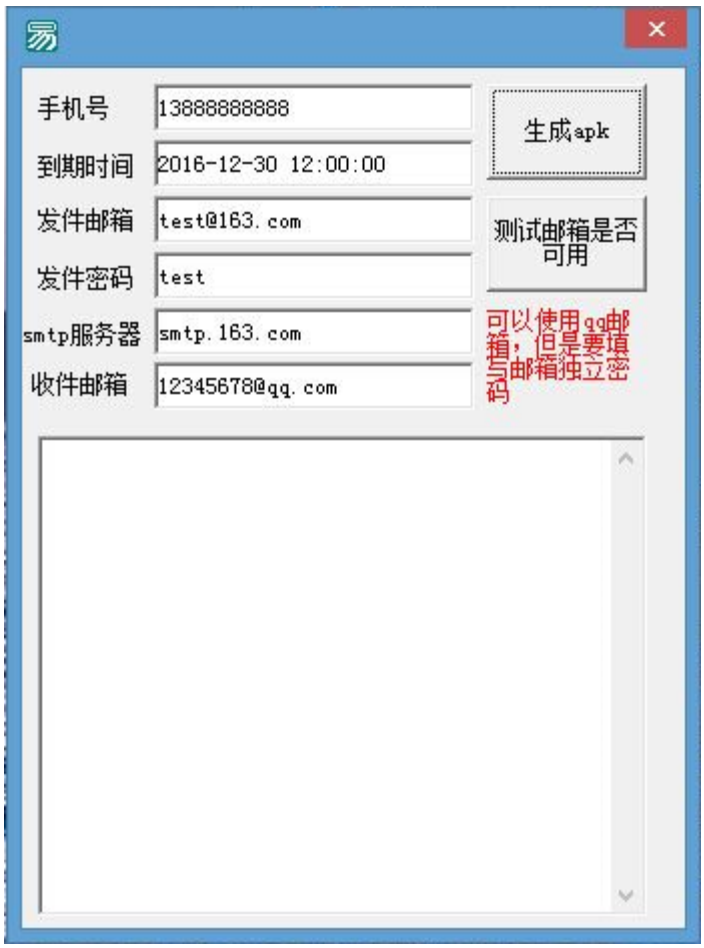


3. 短信拦截木马

”从技术原理和实现上看并不复杂，大多通过注册短信广播（BroadcastReceiver）或者观察模式（ContenetObserver）监控手机短信的收发过程，当然也出现一些功能更全面强大的远控类手机木马，短信拦截之中的一项功能。网上类似的短信拦截源码也非常多，了解过安卓开发的都可以很快编写出一个“短信拦截马”，这也是“短信拦截马”变种速度快、传播泛滥的一个重要原因。

目前我们调查中遇到有两种，一种由编译好的软件填入手机号、发件邮箱账号密码、收件邮箱、木马到期时间即可自动生成一个带有木马病毒的手机 APP。（成本小但是利益大，使用无限制，只要利用生成器就可以制作拦截马，导致拦截马泛滥。）

另一种相当于 PC 版中的远程控制软件一样，由一个控制端也叫服务端（由“钓鱼者”控制）和一个受控端也叫客户端（受害人安装的手机 APP)组成，然后“钓鱼者”就可以控制受害人的手机。

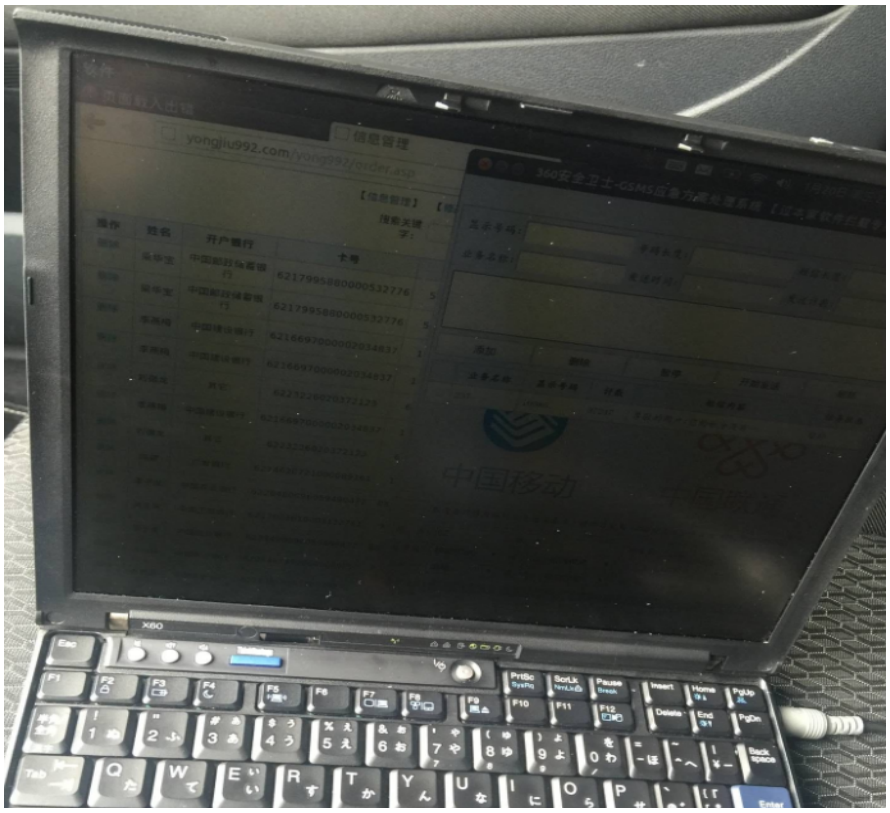


4. 伪基站群发

域名、网站、木马，都准备好了，他们会找伪基站把钓鱼网站在繁华的街区散发出去。

“伪基站”即假基站，设备一般由主机和笔记本电脑组成，通过短信群发器、短信发信机等相关设备能够搜取以其为中心、一定半径范围内的手机卡信息，通过伪装成运营商的基站，冒用他人手机号码强行向用户手机发送诈骗、广告推销等短信息。

通过对 qq 群搜索就会出现很多相关的伪基站贩卖群



注意注意

1.基站代发，诚信接单，500每小时，现游走湖北。

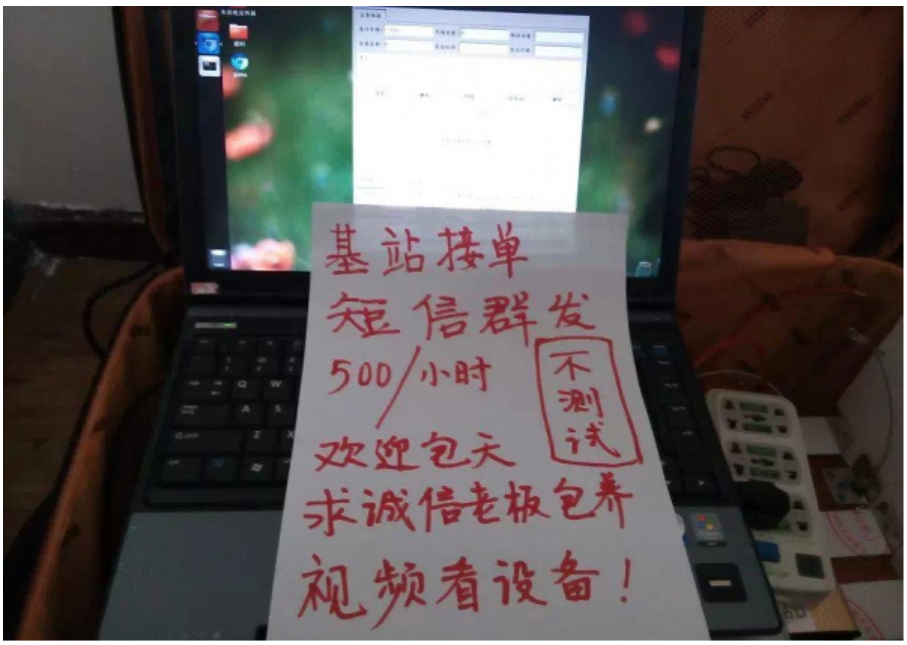
隐藏空白

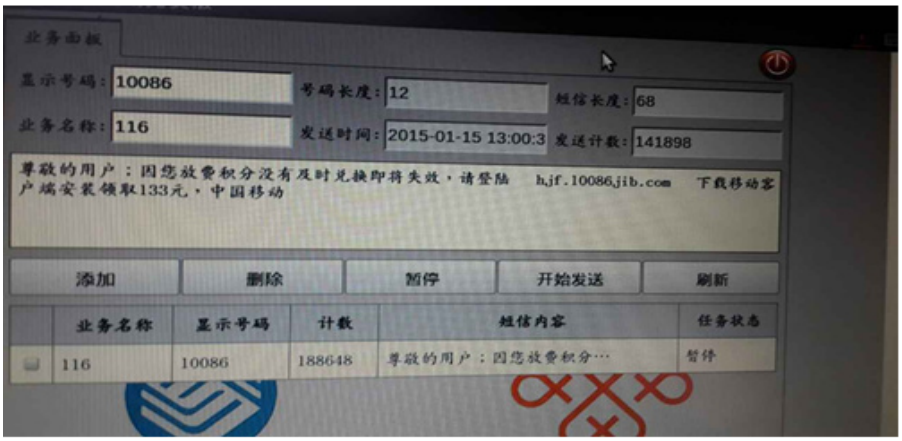
2.淘宝刷单[illegible]款，秒网银马子出售

3.支付宝，通杀余额马子出售。

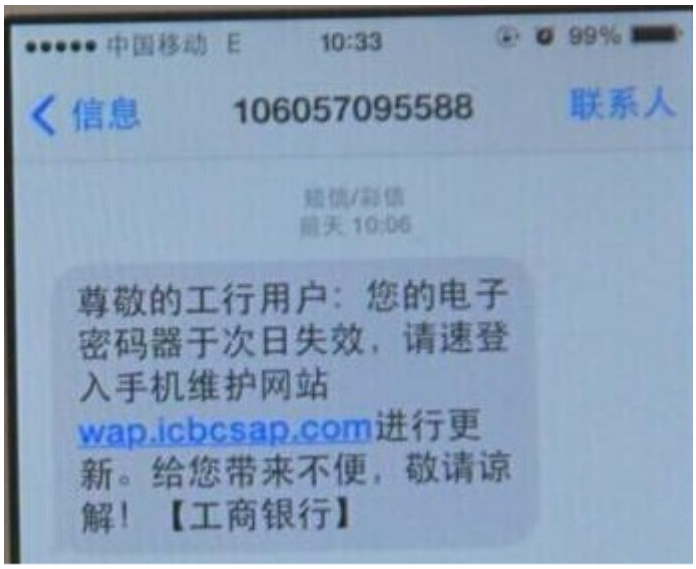
QQ详谈 [redacted]

基站绝对实发，买马的包教会





当人们路过繁华的街区就会收到类似的钓鱼短信



5.“洗料”（盗刷）

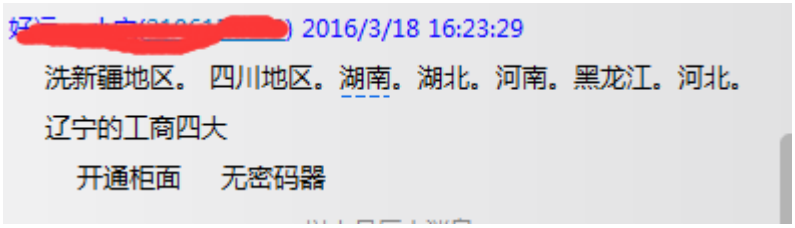
钓鱼者坐等受害者“上钩”在这现在这个互联网发达交易便捷的时代有了你手机的权限，和银行卡账户密码，即可通过快捷支付方式将你的钱财转走。有些没开通网银的受害者的卡他们也会有办法的。

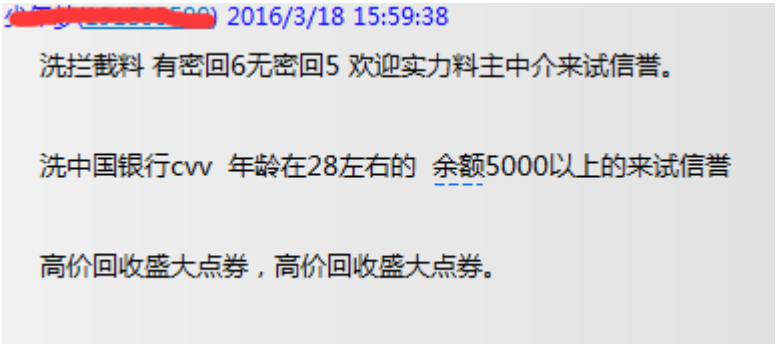
钓鱼者将获取的姓名、证件号码、银行卡号、银行密码、手机号码即被称为“四大件”

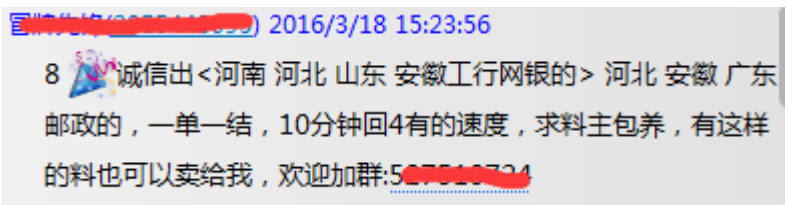
在这些无法被快捷支付的“四大件”（料）

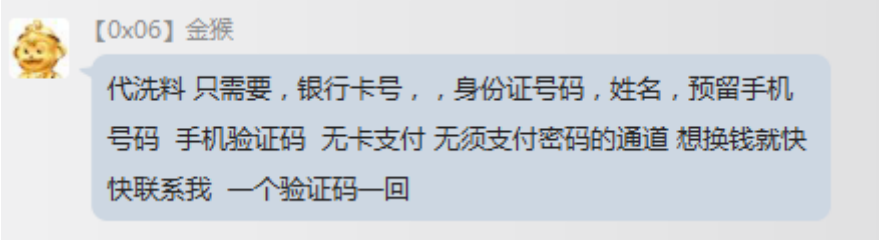
就会将受害者的个人信息进行叫卖，或者找洗料通道（**由于国内各类混乱的支付渠道缺乏有效安全监管，导致黑产团伙一般是通过银行、商户或者第三方支付的各类快捷支付渠道将用户卡内资金转走，他们会购买游戏币、彩票、话费充值、机票门票等多种多样的洗料方法。有些信用卡 CVV 码泄漏的用户还发现通过境外消费渠道被划走资金。有些被感染手机可能还会被订阅一些恶意扣费服务**

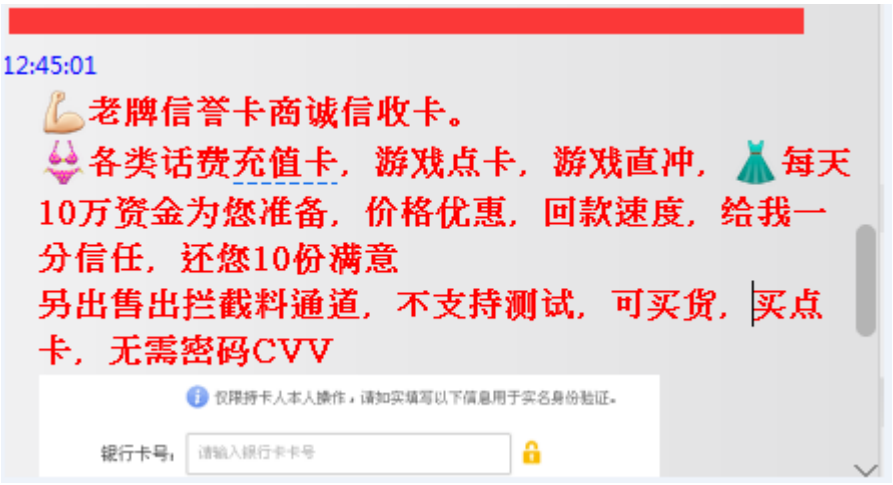
或者使用手机话费支付购买游戏点卡后再进行销赃）进行利益最大化。



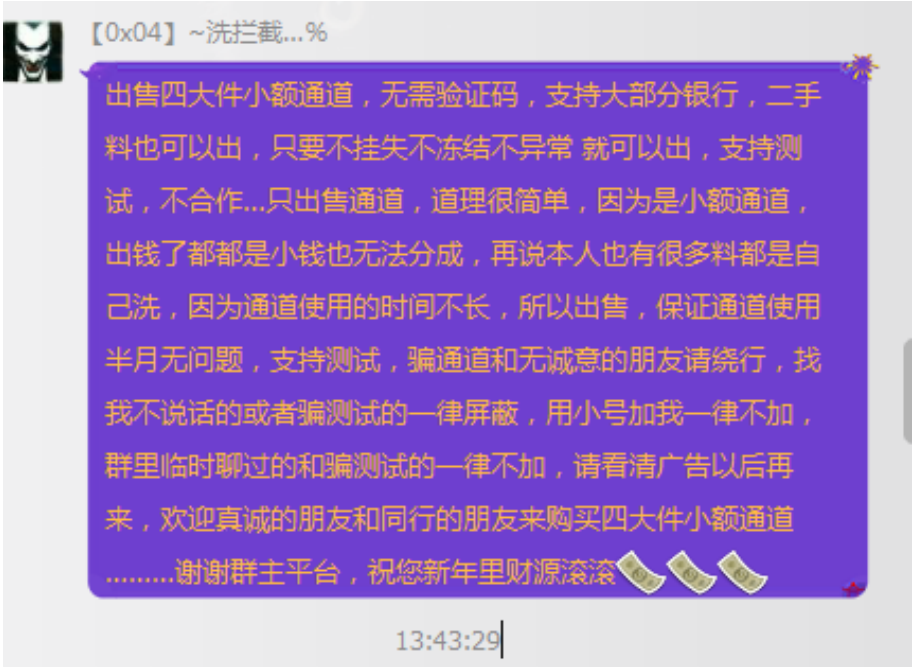





【0x06】金猴
代洗料 只需要，银行卡号，，身份证号码，姓名，预留手机号码 手机验证码 无卡支付 无须支付密码的通道 想换钱就快快联系我 一个验证码一回


12:45:01
老牌信誉卡商诚信收卡。
各类话费充值卡，游戏点卡，游戏直冲，每天10万资金为您准备，价格优惠，回款速度，给我一分信任，还您10份满意
另出售出拦截料通道，不支持测试，可买货，买点卡，无需密码CVV
仅限持卡人本人操作，请如实填写以下信息用于实名身份验证。
银行卡号：
请输入银行卡卡号


2016/3/21 9:26:21
正规银行降级机，秒出复合储-复合信及纯磁料。点位底。欢迎联系合作。 信誉回款截图可供查询，招商转帐记录可供查询真实性。寻料主长久合作。
QQ
【代洗拦截料，储信均可，有密不限额，秒结算回款】



以工商为例只要可以用验证码与“四大件”完成得即可成为被变现的途径。

下面是某洗料群的讨论那个银行好变现。

工商银行服务条约，拥有手机短信权限和银行卡号与密码可利用下面这些业务。

融 e 联

业务简述

融e联客户端软件是我行自主研发的，向个人客户提供移动金融服务的手机客户端软件，具有“消息”、“发现”、“服务”及“我”四大功能，支持跨通信运营商、跨手机操作系统的即时通讯平台。通过该软件客户不仅可以向我行客户经理、客户服务等服务号及其他联系人发送图文信息进行联络沟通，还能发送朋友圈、办理转账汇款等，满足客户信息交流、分享及业务办理等多种需求。

客户端下载

[返回页首]

主要功能

（一）消息

点击“消息”页签可显示您的会话列表，同时您可通过此功能进行聊天发起、好友添加、通讯录查看等操作；

（二）发现

点击“发现”页签您可查看朋友圈及各类信息资讯；

（三）功能

点击“功能”页签您可查询工银信使消息、使用手机银行、融e购客户端等多项服务；

（四）我

点击“我”页签您可查询和设置个人信息。

[返回页首]

适用对象

适用于我行柜面或自助注册的电子银行实名客户，及使用手机号码快速注册的非实名客户。

[返回页首]

工行 e 支付功能

特色优势

1、丰富的业务办理渠道：门户网站、个人网银、手机银行、柜面等多种渠道均可办理。

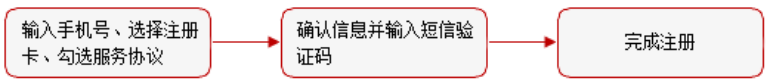
2、统一的账户体系管理：您名下全部工银e支付卡和账户都使用同一手机号码，共享单笔、日累计、月累计等各类支付限额，实现各支付卡限额的统一管理。

3、方便快捷的办理流程：只需三步（输入客户信息、填写验证码、完成确认）即可便捷开通，并为您提供通过个人网银、手机银行渠道批量开通工银e支付功能，方便快捷。

4、统一灵活的风险控制：月累计支付限额为50000元，有效控制支付风险。根据您的自身情况，您可以灵活自助调整单笔、日累计支付限额，并面向U盾客户提供上调更高单笔、日累计支付限额功能。

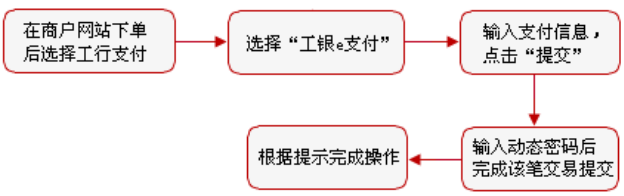
[返回页首]

开通流程



[返回页首]

操作指南



[返回页首]

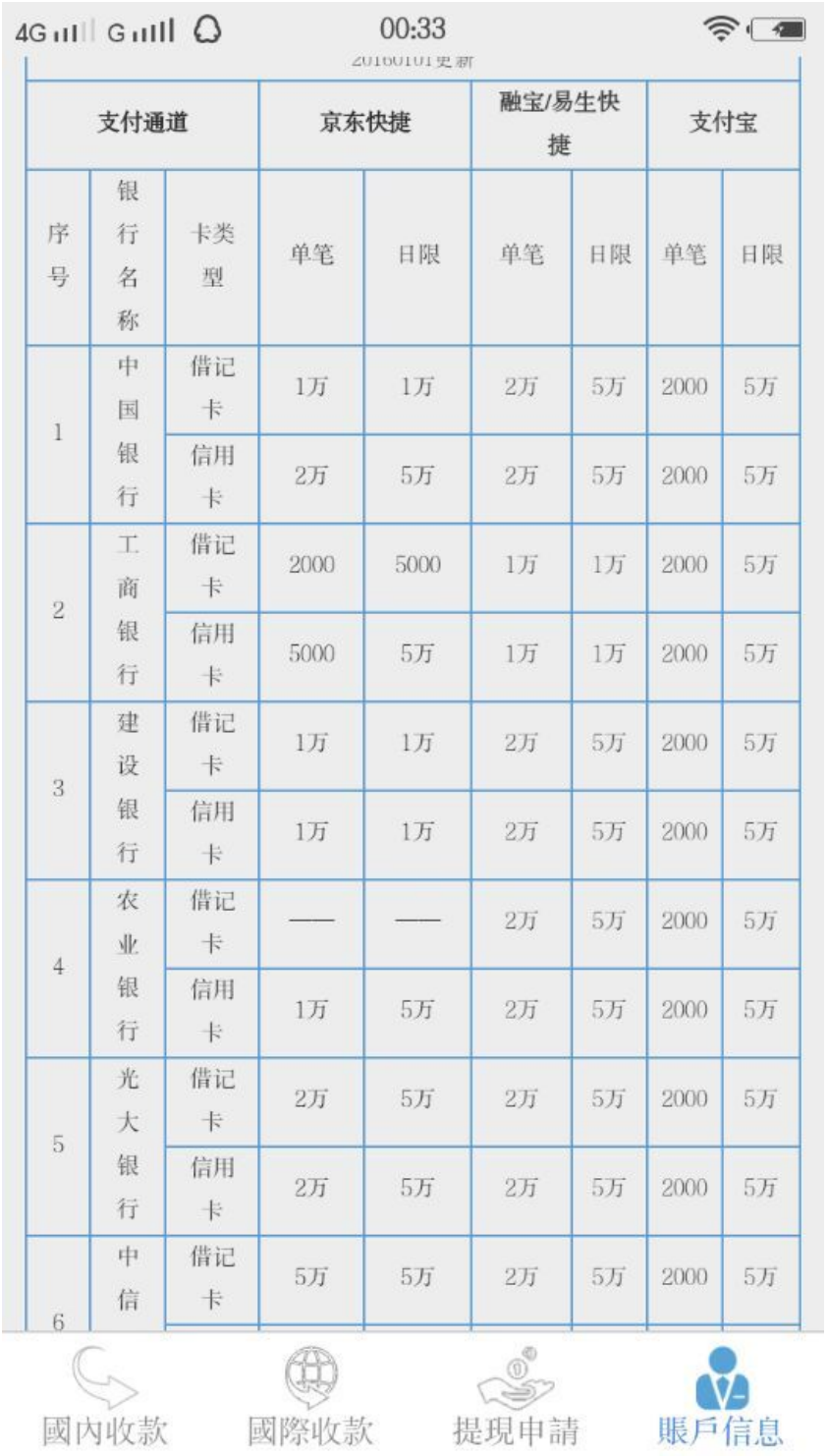
工行快捷支付注意事项：

注意事项

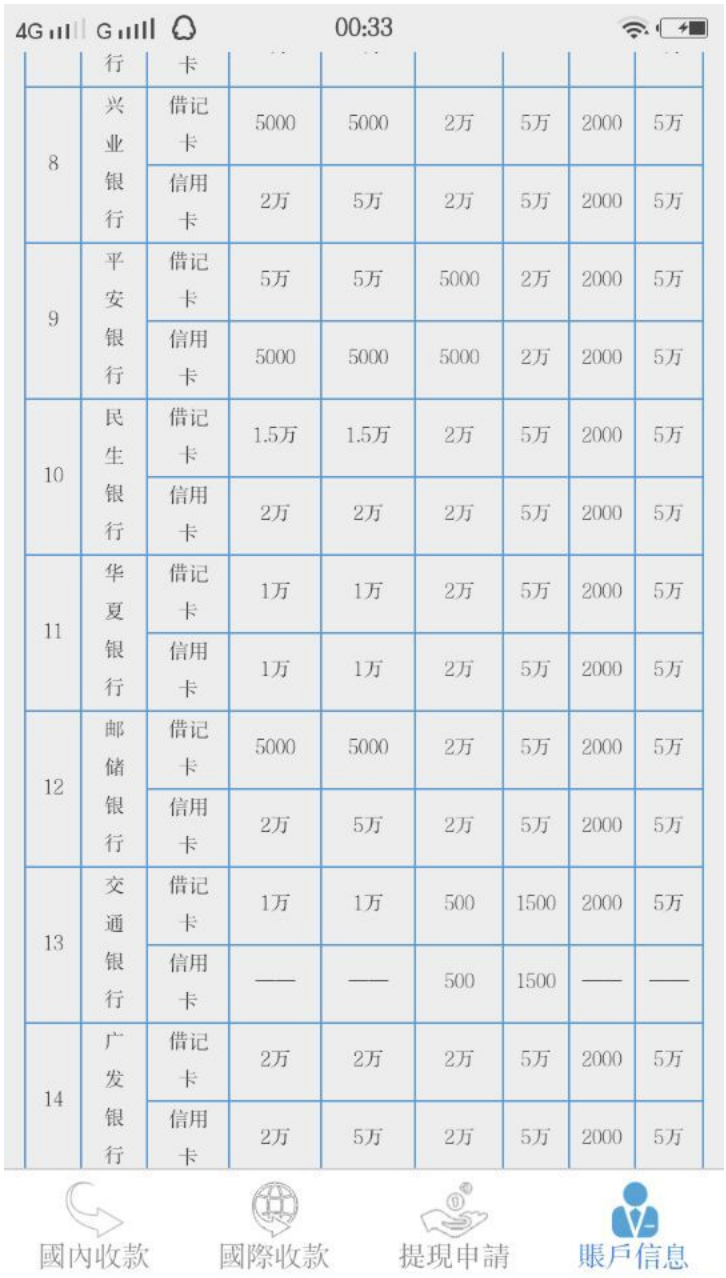
1. 双币贷记卡账户可以作为转入账户和转出账户，但不支持透支转账。
2. 您在进行批量支付时，如果提交与当日提交的指令中有相同总金额、相同总笔数的批量转账汇款时，系统会提示您，避免重复提交。
3. 网上银行“转账汇款查询”和“批量指令查询”功能仅供查询您在网上银行办理的转账汇款的交易信息，暂不能查询通过其他渠道完成的转账汇款业务。
4. 若网上银行付款人在转账汇款时选择“不允许收款人查询此笔交易的收款账号”，当收款账户为个人账户时，收款人查询收款信息时将看不到付款人的账号信息；当收款账户为对公账户时，收款人查询收款信息时将不受限制。
5. 电话银行办理添加“异地卡/账户”无需持“异地卡/账户”，异地账户（不论是您本人还是他人的）只能转入，不能转出。
6. 进行外币转账汇款时，外币“钞户”、“汇户”均可以转入人民币贷记卡，但是从人民币贷记卡中只能转出“钞户”。
7. 根据国家外汇管理局有关规定，外币转账汇款，只能向您同一开户地区的本人账户进行。单笔转账汇款、转账汇款查询支持信用卡外币账户。
8. 通过网银进行单笔转账汇款交易金额低于5,000,000元的实时到账，单笔转账汇款交易金额超过5,000,000元（含）的及时到账。
9. 目前工行转账汇款功能暂不支持运通商务卡和公司运通卡。
10. 对于特定的收款人允许您设置免签名，在一定限额内无需使用电子银行介质认证即可进行交易。

[返回页首]

以下是一些通道的限额，洗料者一般会先转账获得现金，当通道内现金转账达到限额后就会购买商品的方式再将余额消费掉。

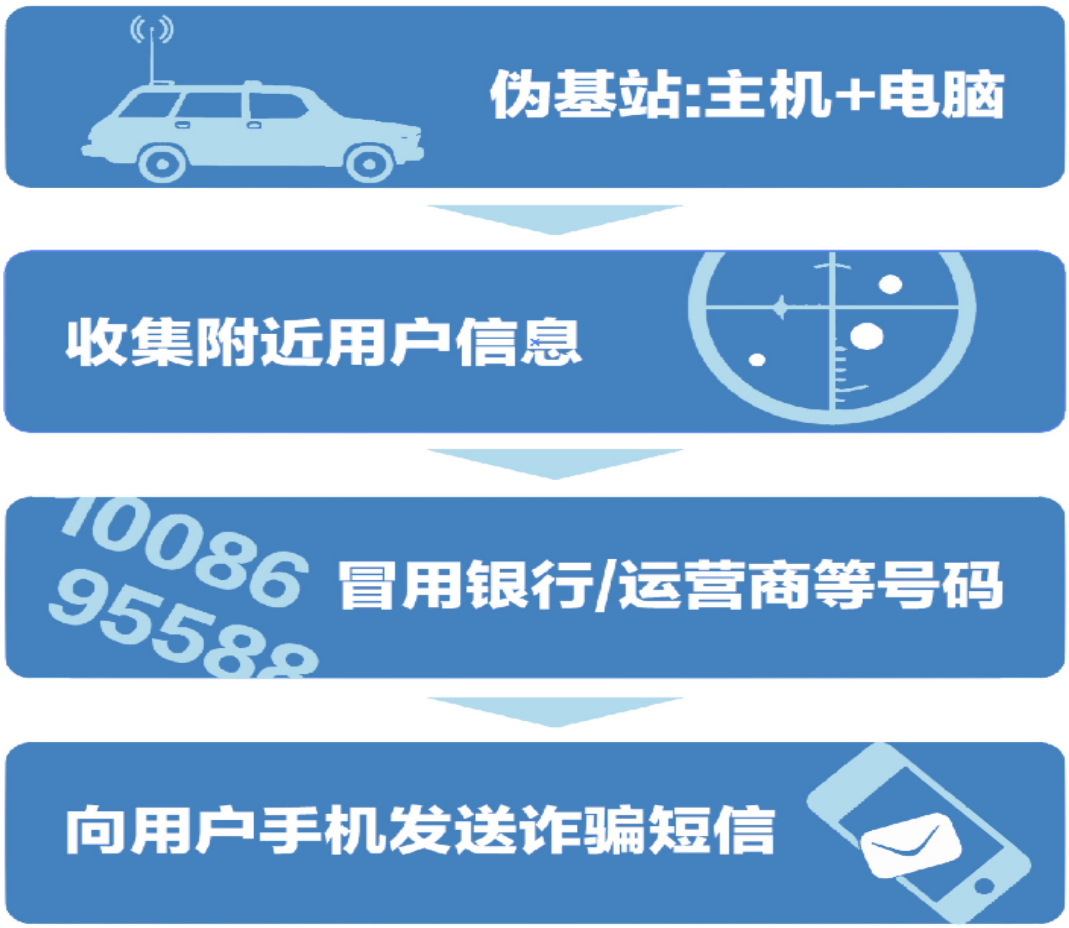


支付通道			京东快捷		融宝/易生快捷		支付宝	
序号	银行名称	卡类型	单笔	日限	单笔	日限	单笔	日限
1	中国银行	借记卡	1万	1万	2万	5万	2000	5万
		信用卡	2万	5万	2万	5万	2000	5万
2	工商银行	借记卡	2000	5000	1万	1万	2000	5万
		信用卡	5000	5万	1万	1万	2000	5万
3	建设银行	借记卡	1万	1万	2万	5万	2000	5万
		信用卡	1万	1万	2万	5万	2000	5万
4	农业银行	借记卡	——	——	2万	5万	2000	5万
		信用卡	1万	5万	2万	5万	2000	5万
5	光大银行	借记卡	2万	5万	2万	5万	2000	5万
		信用卡	2万	5万	2万	5万	2000	5万
6	中信	借记卡	5万	5万	2万	5万	2000	5万



钓鱼网站反制案例

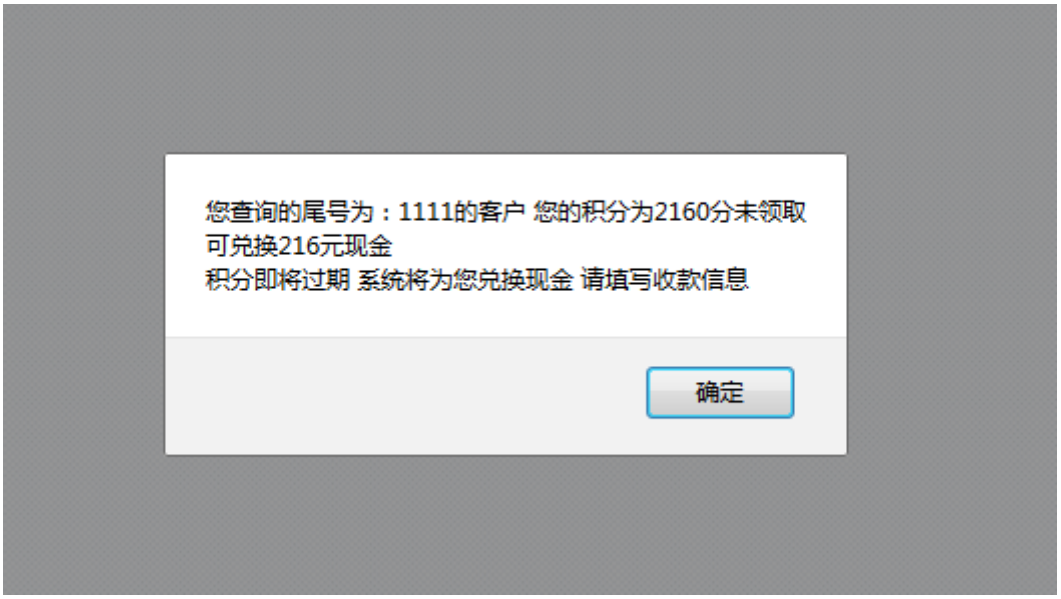
下面两个案例是根据截获到的两个钓鱼网站进行反制



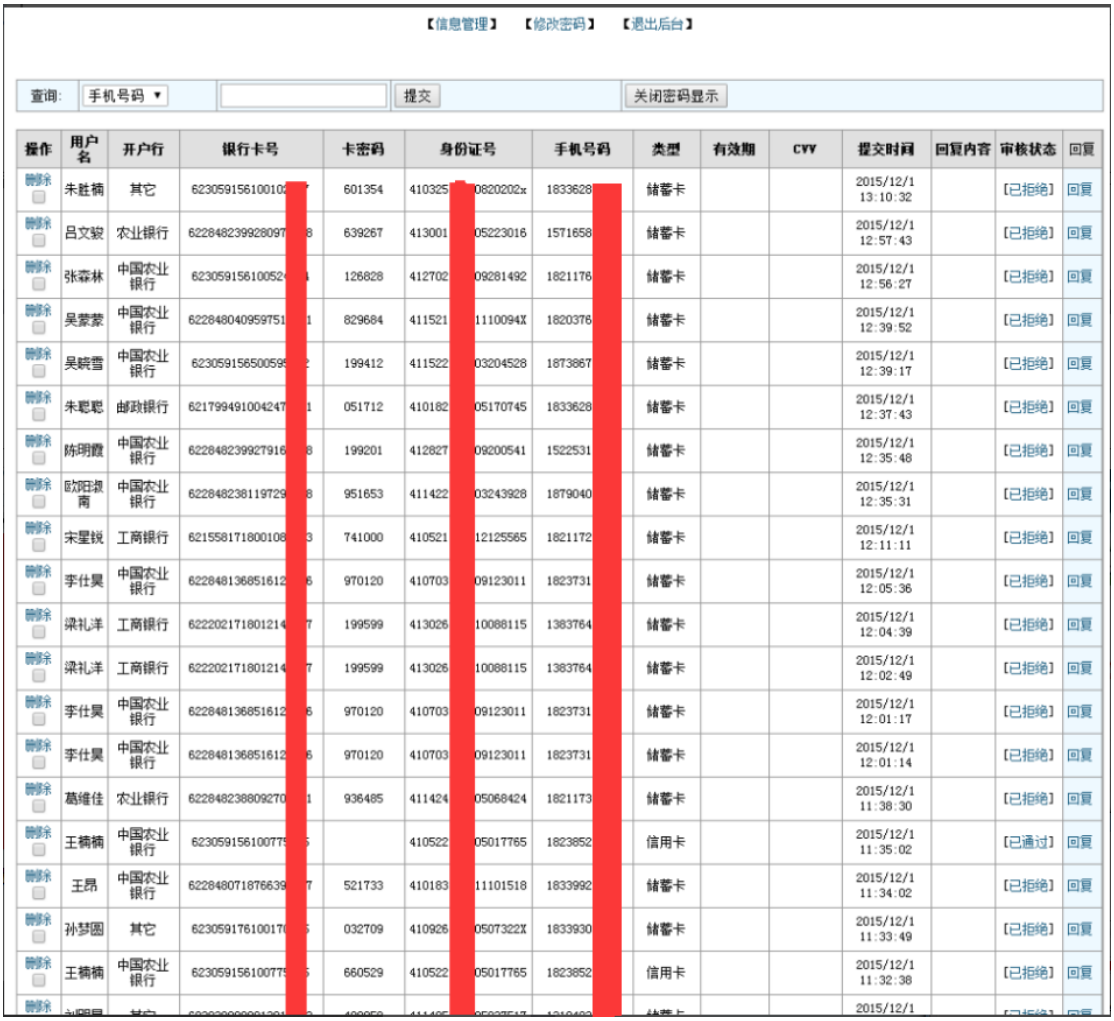
案例一

该网站模仿中国移动网站 ,进入让受害者输入手机号码查询是否可以领取积分兑换现金

输入手机号就会提示您可以兑换现金

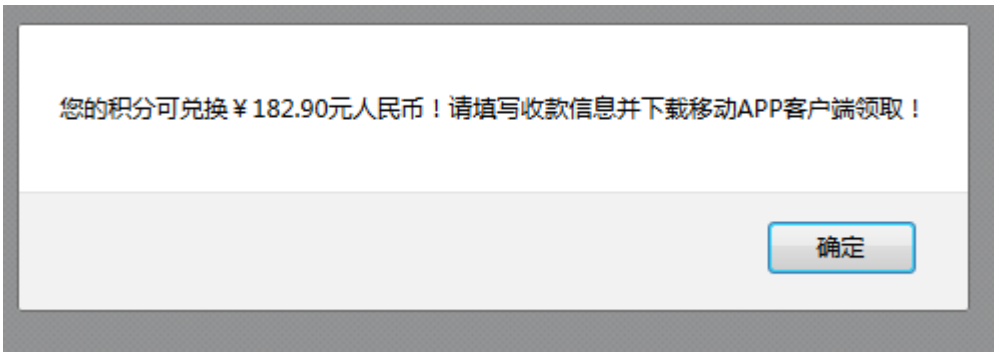


当受害者输入自己的信息后就会将数据提交到网站的后台 ,自己的信息就被盗取了



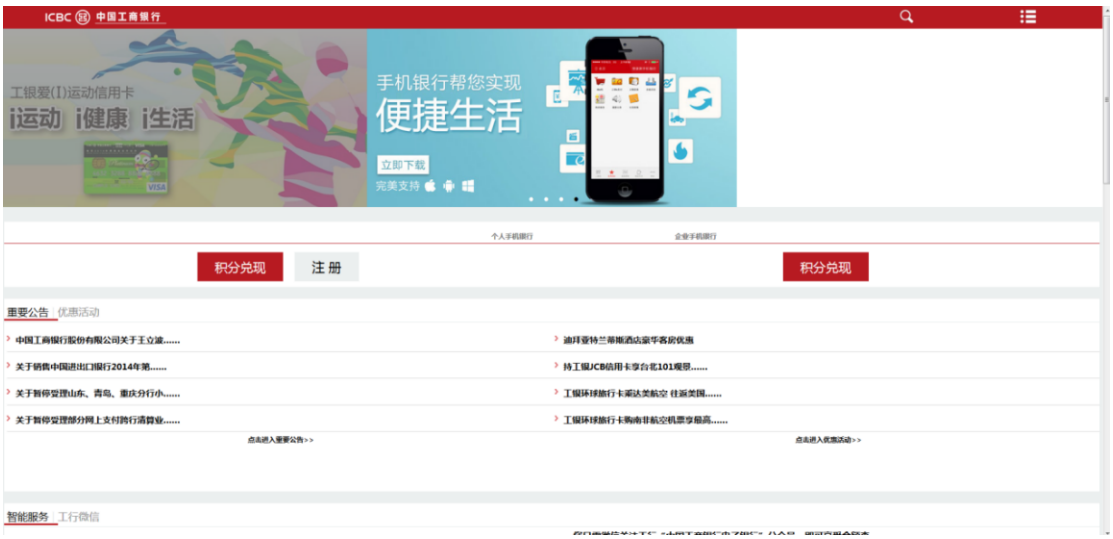
操作	用户名	开户行	银行卡号	卡密码	身份证号	手机号码	类型	有效期	CVV	提交时间	回复内容	审核状态	回复
删除	朱胜楠	其它	623059156100102[redacted]	601354	410325[redacted]0820202x	1833628[redacted]	储蓄卡			2015/12/1 13:10:32		【已拒绝】	回复
删除	吕文骏	农业银行	622848239928097[redacted]	639267	413001[redacted]05223016	1571658[redacted]	储蓄卡			2015/12/1 12:57:43		【已拒绝】	回复
删除	张森林	中国农业银行	623059156100524[redacted]	126828	412702[redacted]09281492	1821176[redacted]	储蓄卡			2015/12/1 12:56:27		【已拒绝】	回复
删除	吴蒙蒙	中国农业银行	622848040959751[redacted]	829684	411521[redacted]1110094X	1820376[redacted]	储蓄卡			2015/12/1 12:39:52		【已拒绝】	回复
删除	吴皖雪	中国农业银行	623059156500599[redacted]	199412	411522[redacted]03204528	1873867[redacted]	储蓄卡			2015/12/1 12:39:17		【已拒绝】	回复
删除	朱聪聪	邮政银行	621799491004247[redacted]	051712	410182[redacted]05170745	1833628[redacted]	储蓄卡			2015/12/1 12:37:43		【已拒绝】	回复
删除	陈明霞	中国农业银行	622848239927916[redacted]	199201	412827[redacted]09200541	1522531[redacted]	储蓄卡			2015/12/1 12:35:48		【已拒绝】	回复
删除	欧阳淑南	中国农业银行	622848238119729[redacted]	951653	411422[redacted]03243928	1879040[redacted]	储蓄卡			2015/12/1 12:35:31		【已拒绝】	回复
删除	宋星锐	工商银行	621558171800108[redacted]	741000	410521[redacted]12125565	1821172[redacted]	储蓄卡			2015/12/1 12:11:11		【已拒绝】	回复
删除	李仕昊	中国农业银行	622848136851612[redacted]	970120	410703[redacted]09123011	1823731[redacted]	储蓄卡			2015/12/1 12:05:36		【已拒绝】	回复
删除	梁礼洋	工商银行	622202171801214[redacted]	199599	413026[redacted]10088115	1383764[redacted]	储蓄卡			2015/12/1 12:04:39		【已拒绝】	回复
删除	梁礼洋	工商银行	622202171801214[redacted]	199599	413026[redacted]10088115	1383764[redacted]	储蓄卡			2015/12/1 12:02:49		【已拒绝】	回复
删除	李仕昊	中国农业银行	622848136851612[redacted]	970120	410703[redacted]09123011	1823731[redacted]	储蓄卡			2015/12/1 12:01:17		【已拒绝】	回复
删除	李仕昊	中国农业银行	622848136851612[redacted]	970120	410703[redacted]09123011	1823731[redacted]	储蓄卡			2015/12/1 12:01:14		【已拒绝】	回复
删除	葛维佳	农业银行	622848238809270[redacted]	936485	411424[redacted]05068424	1821173[redacted]	储蓄卡			2015/12/1 11:38:30		【已拒绝】	回复
删除	王楠楠	中国农业银行	623059156100775[redacted]		410522[redacted]05017765	1823852[redacted]	信用卡			2015/12/1 11:35:02		【已通过】	回复
删除	王昂	中国农业银行	622848071876639[redacted]	521733	410183[redacted]11101518	1833992[redacted]	储蓄卡			2015/12/1 11:34:02		【已拒绝】	回复
删除	孙梦圆	其它	623059176100170[redacted]	032709	410926[redacted]0507322X	1833930[redacted]	储蓄卡			2015/12/1 11:33:49		【已拒绝】	回复
删除	王楠楠	中国农业银行	623059156100775[redacted]	660529	410522[redacted]05017765	1823852[redacted]	信用卡			2015/12/1 11:32:38		【已拒绝】	回复
删除	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]			2015/12/1		[redacted]	[redacted]

当你输入完信息后，还会提示受害者，下载客户端才能激活领取现金，客户端就是经过伪装的木马（后续用来拦截你的交易验证短信）



案例二

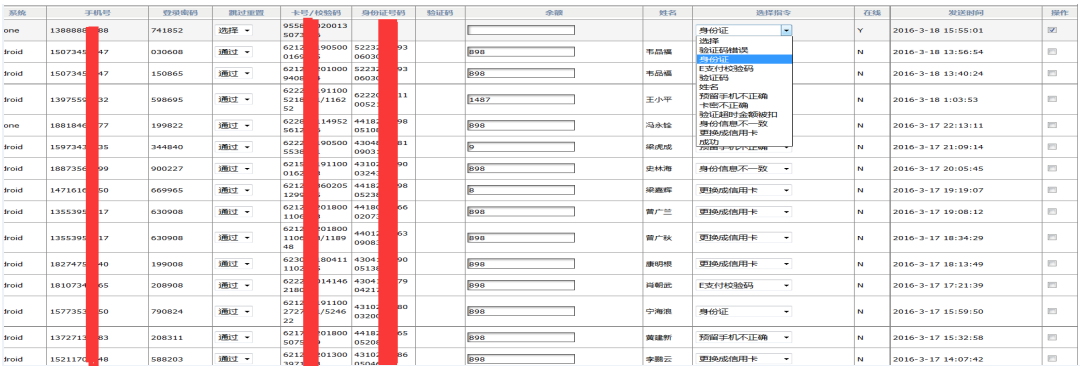
钓鱼网站模仿成中国工商银行



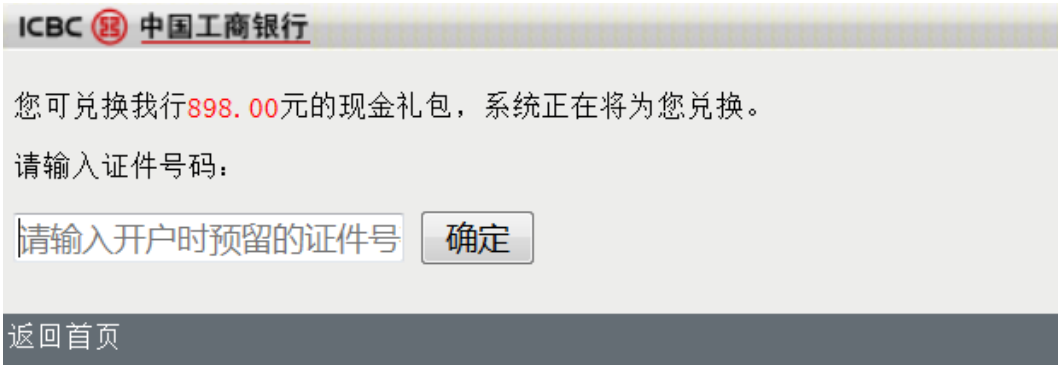
是一个页面让你主动填写您的个人信息

当你点击登录会跳转到指定页面进行等待后台操作者的下一步指令

此时钓鱼者在后台忙碌的操作



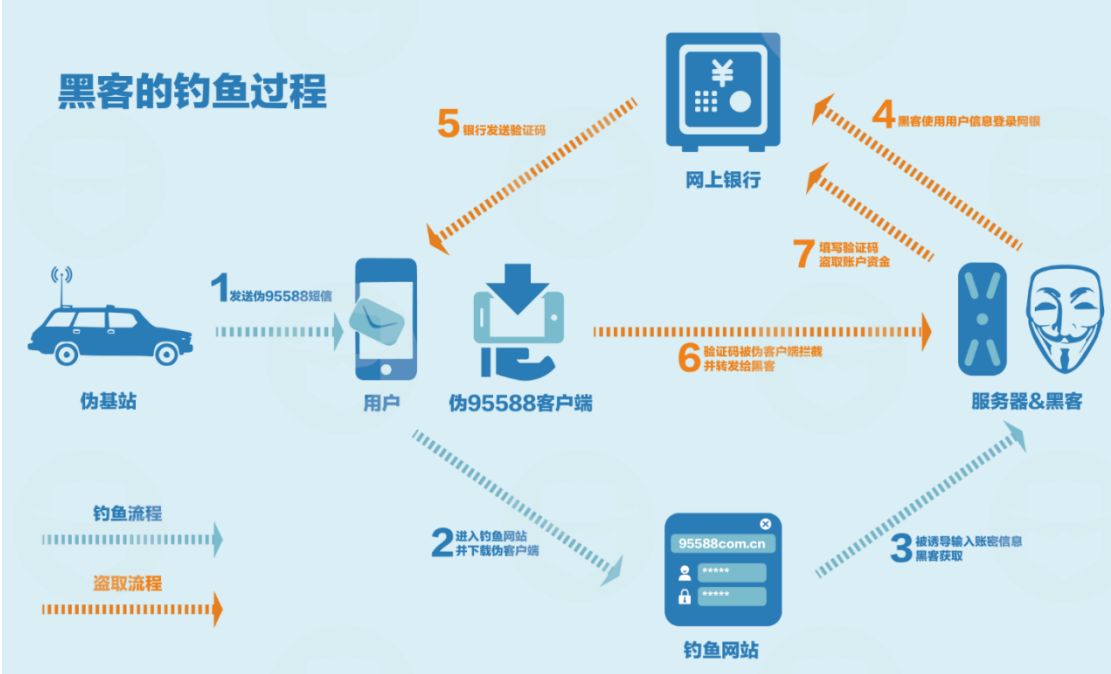
当操作者在幕后提交命令你会进入下一个页面，此时他在诱骗您的身份证信息



操作者提交下一个命令 ,你会跳转到另一个页面此时将要获取您的验证码进行盗刷。

在一步步的操作中受害者的钱财就被盗取了。

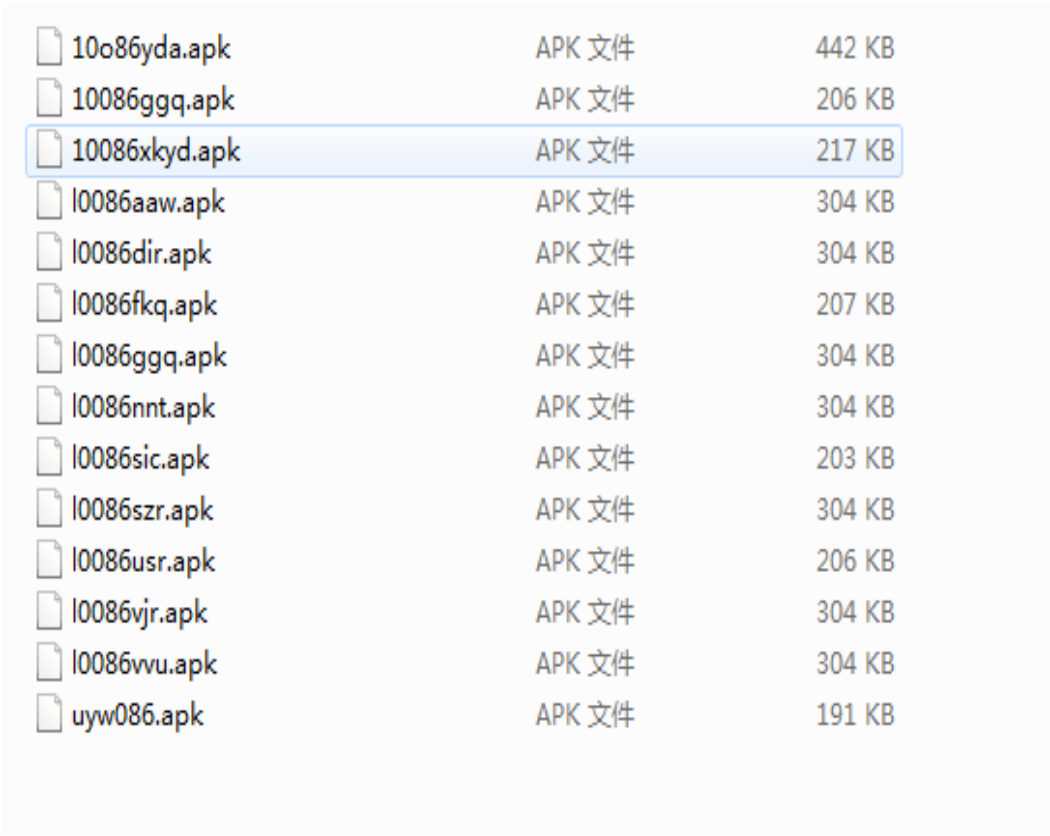
深入调查



该类钓鱼网站通常然后用户输入完个人信息后会提示你下载一个 apk 客户端，

目的就是为了控制受害者的手机，截获短信等内容

我们根据在对这种钓鱼网站中下载的木马进行分析



10o86yda.apk	APK 文件	442 KB
10086ggq.apk	APK 文件	206 KB
10086xkyd.apk	APK 文件	217 KB
l0086aaw.apk	APK 文件	304 KB
l0086dir.apk	APK 文件	304 KB
l0086fkq.apk	APK 文件	207 KB
l0086ggq.apk	APK 文件	304 KB
l0086nnt.apk	APK 文件	304 KB
l0086sic.apk	APK 文件	203 KB
l0086szr.apk	APK 文件	304 KB
l0086usr.apk	APK 文件	206 KB
l0086vjr.apk	APK 文件	304 KB
l0086vvu.apk	APK 文件	304 KB
uyw086.apk	APK 文件	191 KB

```
39      sput-object v0, Lbeckham/owen/util/a;->b:Ljava/lang/String;
40
41      const-string v0, "156789      @163.com"
42
43      sput-object v0, Lbeckham/owen/util/a;->c:Ljava/lang/String;
44
45      const-string v0, "aa899908"
46
47      sput-object v0, Lbeckham/owen/util/a;->d:Ljava/lang/String;
48
49      const-string v0, "1567      1@163.com"
50
51      sput-object v0, Lbeckham/owen/util/a;->e:Ljava/lang/String;
52
53      const-string v0, ""
54
55      sput-object v0, Lbeckham/owen/util/a;->f:Ljava/lang/String;
56
57      const-string v0, "15678      1"
58
59      sput-object v0, Lbeckham/owen/util/a;->g:Ljava/lang/String;
60
61      const-string v0, ""
62
63      sput-object v0, Lbeckham/owen/util/a;->h:Ljava/lang/String;
64
65      const-string v0, "smtp.163.com"
```

此类木马源码中都会留了一个作者的手机号和一个发信邮箱和一个收信邮箱，可以收集受害者的手机通讯录和收发拦截的受害者的信息，从而使用快捷支付功能就会神不知鬼不觉的将受害者的钱财盗取。

通过分析 apk 木马文件得到攻击者的发件邮箱账号密码，登入邮箱，可以发现大量被害用户的手机短信，通讯录内容

----------null 95188----------
2014-07-20 20:09:49 【支付宝】383224（支付宝短信校验码，请勿泄露），需要你进行身份校验。如非本人操作，请致电95188。
2014-08-05 17:23:08 【支付宝】你的支付宝发生285.62元的交易，校验码：948811打死都不能告诉别人哦！唯一热线95188
2014-08-20 12:38:09 【支付宝】你的支付宝发生195.00元的交易，校验码：903238打死都不能告诉别人哦！唯一热线95188
2014-08-29 17:27:05 【支付宝】你的支付宝发生1110.04元的交易，校验码：778156打死都不能告诉别人哦！唯一热线95188
2014-09-11 21:21:44 【支付宝】你的支付宝发生304.00元的交易，校验码：515115打死都不能告诉别人哦！唯一热线95188
2014-09-25 08:58:23 【支付宝】你的支付宝发生422.20元的交易，校验码：902177打死都不能告诉别人哦！唯一热线95188
2014-09-25 12:56:15 【支付宝】你的支付宝发生866.00元的交易，校验码：125801打死都不能告诉别人哦！唯一热线95188
2014-09-26 21:20:58 【支付宝】你的支付宝发生1196.00元的交易，校验码：563513打死都不能告诉别人哦！唯一热线95188
2014-10-16 20:09:55 【支付宝】短信校验服务费0.60元已扣款(银行卡尾号7805)，下次扣款时间2014-11-16。
2014-10-20 20:22:24 【支付宝】532631（支付宝短信校验码，请勿泄露），需要你进行身份校验。如非本人操作，请致电95188。
2014-10-20 20:22:39 【支付宝】532631（支付宝短信校验码，请勿泄露），需要你进行身份校验。如非本人操作，请致电95188。
2014-11-02 14:12:21 【支付宝】782015（支付宝短信校验码，请勿泄露），需要你进行身份校验。如非本人操作，请致电95188。
2014-12-10 13:00:20 【支付宝】你的支付宝发生49.00元的交易，校验码：750841打死都不能告诉别人哦！唯一热线95188
2014-12-12 15:10:58 【支付宝】你的支付宝发生370.00元的交易，校验码：525297打死都不能告诉别人哦！唯一热线95188
2015-01-22 12:49:32 【支付宝】你的支付宝正在变更账户信息，校验码：916998，打死都不能告诉别人哦！唯一热线95188
2015-12-18 23:25:30 【支付宝】你的支付宝正在发生699.00元的交易，校验码：848257，打死都不能告诉别人哦！唯一热线95188

全部短信(863598020072970)

wenzhenwu990

发给 wenzhenwu990　　2016-03-16 12:01 详细信息

----------0 10086----------
2016-02-15 20:32:25 尊敬的客户：您的资费套餐免费通话分钟在02月15日20时32分前已使用完毕，敬请留意。中山移动
2016-02-19 21:59:08 尊敬的客户，如需了解腾讯业务，请用手机登陆[3g.qq.com]或[wap.3g.qq.com]，电脑登陆：[www.qq.com]，手机登陆网站按各品牌手机流量资费标准收取。
2016-02-19 21:59:13 尊敬的客户，如需咨询腾讯业务，请用手机登陆[kf.3g.qq.com]，电脑登陆腾讯互联网：[http://service.qq.com]，或致电客服电话：0755-83763333。温馨提醒：拨打该电话按现行各品牌资费标准收取，手机登陆网站按各品牌手机上网资费标准收取。
2016-02-22 09:40:43 尊敬的客户，为您赠送的30天1G省内4G专用流量免费体验包即将到期。若您觉得意犹未尽，推荐回复BLSJLL了解更多适合你的流量套餐。中国移动
2016-02-24 15:12:06 尊敬的客户：您已于2016年2月24日成功存入20.00元,感谢您的使用，中国移动广东公司。
2016-03-10 17:06:19 尊敬的客户：您2016年2月的总话费为107.70元。查询余额、欠费及需缴话费请本机拨打1008611，电脑登录 gd.10086.cn 可查询详细账单以及充值缴费。如有疑问或需帮助，请回复0咨询在线客服。中国移动
2016-03-13 11:37:33 尊敬的客户：为了让您节省话费及更安心地使用本号码，现开展“交话费，全年电话任打，流量任用，再送1年高速宽带”活动，欲了解更多详情，请发送818至10086了解。回复0寻求客服帮助。中国移动
2016-03-13 11:39:24 818
2016-03-13 11:39:40 尊敬的客户：2016年4月30日前，您只需交500元话费，可享受一年内电话任打、流量任用优惠，再送一年宽带。请前往沟通100服务厅、移动网点办理；或在同一天内一次性或累计通过广东移动10086手机客户端、微信、支付宝等方式完成充值，并发BL818到10086登记。注：1、活动需承诺使用1年的38元飞享套餐。2、全球通客户根据当月消费金额每月赠送话费；预付费客户所交话费立即到账，赠送话费按消费情况提前或于第7个月一次性到账。活动所有话费（所交话费+赠送话费），有效期一年。3、本活动要求当月完成实名登记、更换为4G卡、在非欠费状态下参加；4、任用封顶为1500元（含所交话费），包括国内通话费、国内流量费、基本月套餐费。如有疑问或需帮助，请回复0咨询在线客服。中国移动
2016-03-16 11:40:01 尊敬的用户：因您话费积分没有兑换即将清零，请登陆 wap.uyr0086.com 按提示兑换216.00元礼包【中国移动】

----------0 106350096138----------
2016-02-18 12:35:11 【广东农信】您尾数9091的卡号02月18日12时35分收入人民币1500.00元(ATM存款),余额1514.77元【中山农商银行】
2016-02-22 13:46:12 【广东农信】您尾数9091的卡号02月22日13时44分支出人民币180.00元(消费),余额1334.77元【中山农商银行】
2016-02-23 15:24:07 【广东农信】您尾数9091的卡号02月23日15时23分支出人民币150.00元(消费),余额1184.77元【中山农商银行】
2016-02-24 15:12:16 【广东农信】您尾数9091的卡号02月24日15时11分支出人民币17.98元(财付通快捷充),余额1166.79元【中山农商银行】
2016-03-02 21:35:24 【广东农信】您尾数9091的卡号03月02日21时35分支出人民币300.00元(ATM取款),余额861.79元【中山农商银行】
2016-03-09 07:57:46 【广东农信】您尾数9091的卡号03月09日07时57分在自助渠道输入密码连续累计错误1次，如非本人操作，请立即致电客服热线96138或通过网上银行办理临时挂失。【中山农商银行】
2016-03-09 09:32:30 【广东农信】您尾数9091的卡号03月09日09时32分在自助渠道输入密码连续累计错误1次，如非本人操作，请立即致电客服热线96138或通过网上银行办理临时挂失。【中山农商银行】
2016-03-09 09:32:39 【广东农信】您尾数9091的卡号03月09日09时32分支出人民币200.00元(异地跨行取款),余额656.79元【中山农商银行】

我们从拿下的一些钓鱼网站的后台中获取的一些部分信息。

储蓄卡：卡号 密码 姓名 身份证 手机号

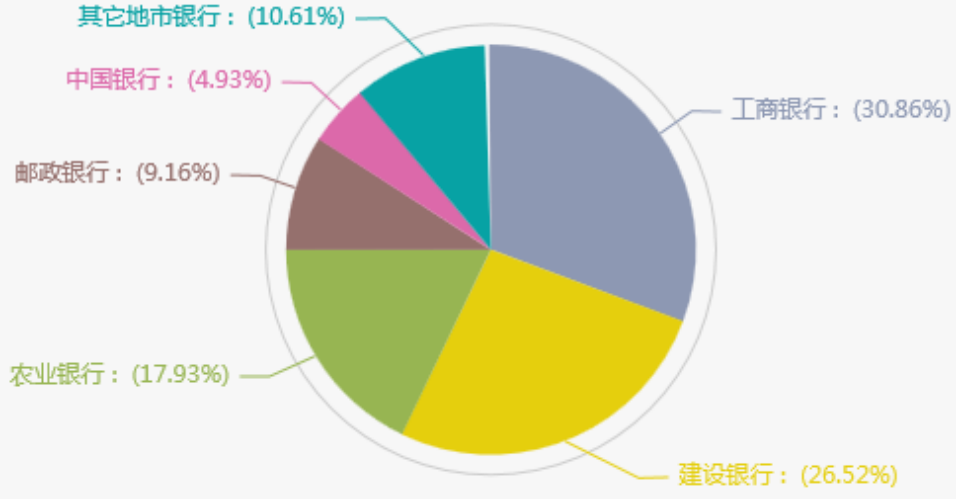
622848033911746	199012	何成光	5325311990100	1885880
621226250201662	613461	张兴全	5322331969061	1375948
622202250201848	131420	陶乃佑	5303811986050	1590880
62122625020166	613461	张兴全	532233196906	1375948
62122624020196	201366	褚光超	522427199511	1351193
62220225020074	102688	李贵发	530128199106	1588716
62122625170022	062729	任惠芬	532401197209	1398777
62122625170023	121115	冯珂豪	530421199212	1575238
6222082502000	678727	李函忆	532425198002	1380873
622202170501	870805	单金阁	410323198709	1583880
621226250201	123789	张浩	511602199701	182146
4895920315	900006	王岩波	230221197206	136748
6214838714	129582	刘潇戈	411481199405	159900
622208250200	723926	王嘉	533222199307	147878
622202250200	355366	李贵发	530128199106	158871
95588025022	663317	吴刘平	532627198204	135187
6222300323	115296	李娜	530402199110	187877
6212262502022	654329	陈树昆	532426196309	138882
62122625160012	666999	王琼	532301196306	158088
62122625020000	026616	胡家婷	532131198109	153983
62122625020230	123458	何宗懂	530381199409	150870
62122625020017	915915	杨刚	530111197809	135770
6222022517000	288066	朱莹莹	532128198206	150088
42702004001	011311	房华	530102197411	138882
621226250200	915915	杨刚	5301111978091	135770
622208250200	668899	计大利	5110281990100	1519896
621226251700	621215	范夫贵	5327011955073	1398862
6212262502022	456856	高翔	5321251986092	13508
6228480868599	530427	缪德龙	530427199810088	150871
62220225050036	096021	陆荣鑫	530328199801	1592473
621226251700193	621215	刘华	532401196201	1303866
621226250202234	456856	高翔	5321251986092	1350871

62122625020182	982512	彭国辉	4304211982100	135187
6222023100063	200009	王忠军	532129199202	157529
62122625050023	200791	王浩然	530322199101	159745
62122625020217	110926	刘艳菊	522729198109	159252
622202310006318	200009	王忠军	532129199202131	157529
621226250200775	769698	陈延河	530129197102	158872
621558250200035	910630	彭坤坤	4209231991063	159251
6222022502015576	118118	顾尚勇	5322241980061221	13908851
6212262502008448	815890	魏忠香	530113197601263	15974815
6212812502001540	125621	周世涛	530128199709244	18787197
6212262502020988	514212	段生念	533023199207072	1317060
6222082502002655	585858	林绍跑	330328196902024	1375910
53099000349098	601859	李树武	230827196609180	1394660
6212262502008584	036782	杨庆	532128199108	18288222
6212262502017522	513418	汤金坤	530326198706	15288495
62148387135685	199799	黄锁	5325251997090	159871398
621226250201157	530128	张德宏	530128199202	151989957
62122625020165	480239	顾伟	530102199203	15911747
25021050010122	256364	耿云碧	530102198803	1375913
6215582516000	804308	陈大刚	532123198201	1596949
621700389000	749193	汪甲尧	530322200	1830874
62128125020	199636	袁海兵	530322199	1588720
621226250202	12345	何宗懂	530381199	1508705
621226250201	010509	张克方	522727198	1500851
6217232517000	751314	普成恩	530427199	1509676
62122625020226	224338	魏天灿	52020219920	1519874
62122625020140	382569	吴现福	530326198606	1365883
622202250200	986727	姜禹波	530129198304	1388849
6214833880568	515478	楚星梅	533222199311	1878765
621281250200149	197118	雷发锐	530326199711	1528829
6212262502016749	910529	覃静	422827199308	156876
6212262502020293	199710	梁多	530324199711	152883
621226250201836	010509	张克方	522727198805	15008
621226250201060	810530	邓华平	511222198111	1588 7
62223003234838	982106	罗杰	530427198308	13759

数据解读

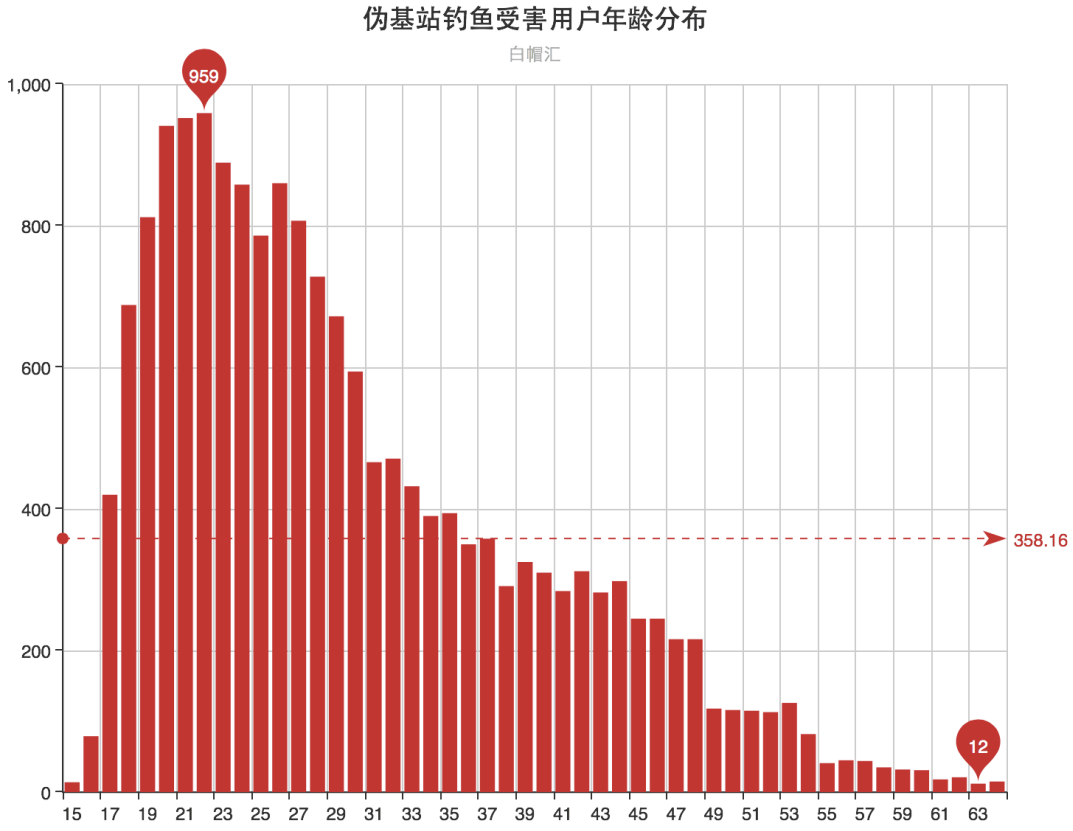
金融账号影响的银行分布

被骗用户所在的开户行根据数据前五名排序分别为：工商银行，建设银行，农业银行，储蓄银行，中国银行。

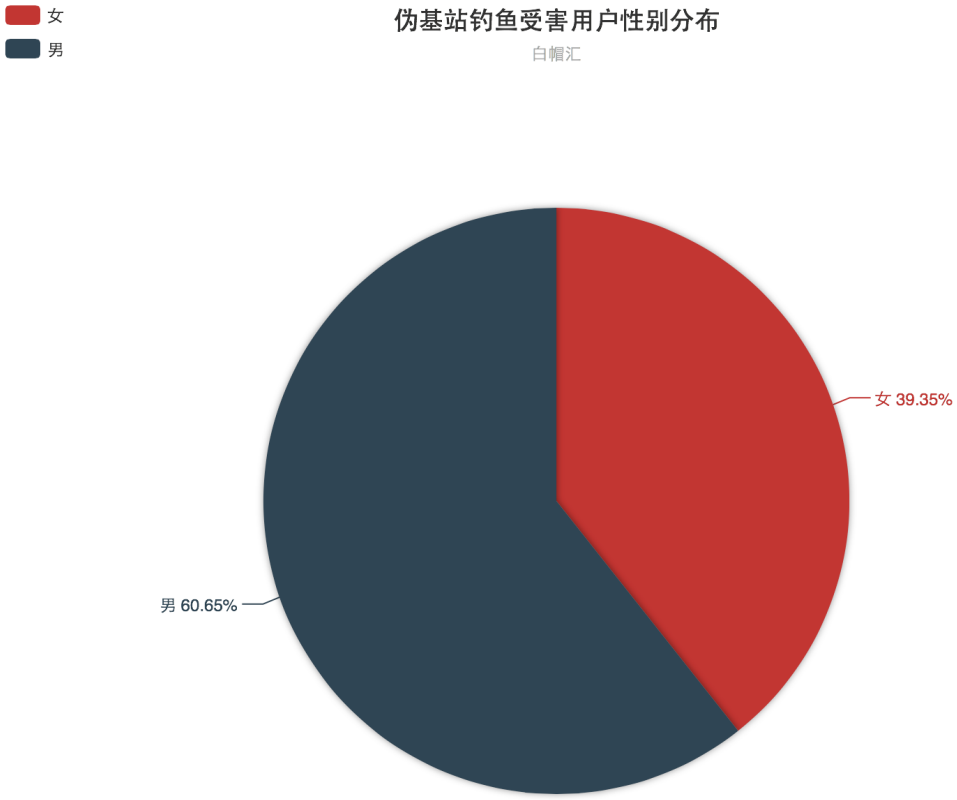


受害人群的年龄段分布

其中受骗人群集中在 19-29 岁的人群，主要分布在 二、三 线城市为主。

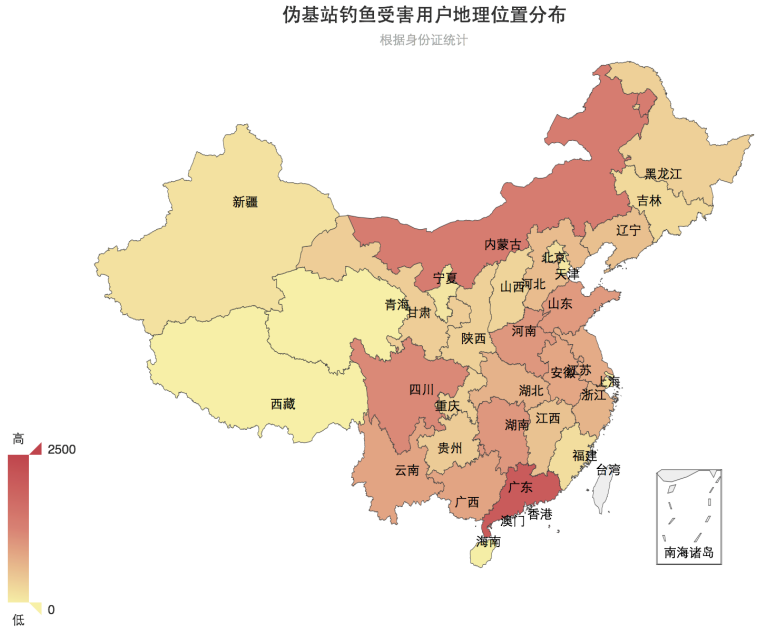

伪基站钓鱼受害用户年龄分布
白帽汇
959
12
358.16
1,000
800
600
400
200
0
15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51 53 55 57 59 61 63

受害人群的性别分布

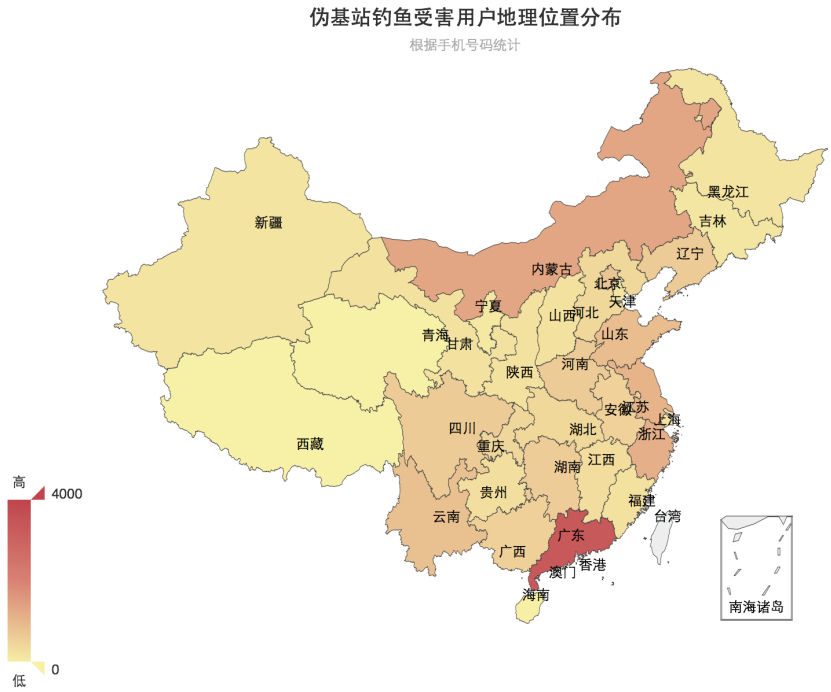


受害人群的地域分布

根据身份证号码的地址归属进行地理位置统计，排名前五位的省份分别是：广东，内蒙古，四川，湖南，河南。



根据手机号码的地址归属进行地理位置统计，排名前五位的省份分别是：广东，内蒙古，浙江，江苏，山东。



应对策略

对此我们提出几点防范意见供参考：

1.用户应加强个人安全防范意识，不要轻信任何中奖信息、轻易点击中奖网站链接。

2.当用户接收到包含网站链接的短信时，需仔细甄别网站的域名，钓鱼网站常常伪装成和真实网站相近的域名 ,如攻击者会使用如1oo86.cn等与10086.cn真实网站接近的域名。

3.用户还需注意保护个人信息，不要在通过点击电子邮件链接访问的网站上输入相关登录账号、密码等信息，也不要在未知的网站上提交个人重要信息。

后续跟进

附录：伪基站短信模板

工商银行：
尊敬的工行用户:您的账户累计积分 xxx 即将逾期清空,请登录 xxx.xxx.xxx 兑换 xxx 元现金【工商银行】
尊敬的工行用户:您的积分已满 xxx 分,登陆手机官网 xxx.xxx.xxx 可兑换 xxx 元现金大礼.逾期清零【工商银行】
尊敬的工行用户：您的账户积分 xxx 即将逾期清空，请登陆兑换网 xxx.xxx.xxx 兑换 xxx 元现金，逾期失效【工商银行】
尊敬的用户：我行将开展个人信息核实认证，请登录 xxx.xxx.xxx 按提示核实，未核实账户将于今日 24 点冻结【工商银行】
尊敬的工行用户：您的账户积分 27347 即将逾期清空，请及时访问 wap.icbytp.com 进行兑换 1367.35 元现金【工商银行】
尊敬的工行网银用户：您的工行网银电子密码器将于次日失效，请及时登录 xxx.xxx.xxx 进行升级激活，感谢您对我行的支持【工商银行】

尊敬的工行用户：您的账户未经核实，请及时登录官网 xxx.xxx.xxx 进行身份核实，逾期将冻结账户[工商银行]

中国移动:

尊敬的用户：因您话费积分没有兑换即将清零，请登陆 xxx.xxx.xxx 按提示兑换 xxx 元礼包【中国移动】

尊敬的用户: 您话费积分已满 xxx 可兑换 xxx 元现金礼包,请登陆 xxx.xxx.xxx 激活领取,过期失效 【中国移动】

尊敬的移动用户您好：我公司举行 16 周年庆话费充值活动。充一百送一百，即时到帐，请登录移动掌上营业厅 xxx.xxx.xxx 中国移动

移动周年庆！为回馈老用户，推出充 100 送 300 话费大赠送活动，手机登录 xxx.xxx.xxx 活动期间限充值一次 ！中国移动

建设银行:

尊敬的建行用户:您的建行账户信用额度已满一万积分可兑换 5%的现金，请使用手机登陆 xxx.xxx.xxx 查询兑换逾期失效【建设银行】

尊敬的客户：由于您的账户未核实，现已限制账户支出，请速登入我行 xxx.xxx.xxx 进行登记核实,逾期将注销该账户【建设银行】

尊敬的用户;您的手机银行将于次日失效,请立即登陆建行手机网 xxx.xxx.xxx 进行认证,逾期失效【建设银行】

尊敬的用户：我行将开展个人信息核实认证，请登录 xxx.xxx.xxx 按提示核实，未核实账户将于今日 24 点冻结。【建设银行】

尊敬的建行用户:沈阳建行卡客户领红包了！登陆我行官网 xxx.xxx.xxx 查询领取！【建设银行】

紧急通知:您的建设银行卡即将失效，请登陆我行手机官方网站重新验证，逾期作废处理【建设银行】请立即登陆我行网站 xxx.xxx.xxx

尊敬的用户:您是我行特约用户，您信用卡现可提高永久额度！请于 24 小时内进入 xxx.xxx.xxx 申请，逾期失效【建设银行】

农业银行:

尊敬的农业银行客户您好：我行将于 2016 年 3 月 31 日止，将冻结您名下所以银行帐户，详情请咨询 01089049192《农业银行》

【中国农业银行】通知：截止今日 16:59 将对您个人账户进行冻结，如有疑问详情咨询：02389310152

温馨提示：截止今天 24：00 之前我行将扣除您的农行卡年费 1800 元。如有疑问请致电农行客服中心：4006363392【农业银行】

尊敬的客户：您的农业银行账户因未核实个人身份信息已被停用，请登陆 xxx.xxx.xxx 按提示核实升级解冻

尊敬的用户：您的积分已满 18000 分可兑换 5%的现金请手机登录 xxx.xxx.xxx 查询领取逾期失效【农业银行】

关于我们

北京白帽汇科技有限公司是一家专注于安全大数据、企业威胁情报，为企业提供尖端安全产品和服务的一家高科技互联网企业。

NOSEC大数据安全协作平台（NOSEC.ORG）是其旗下的一款大数据安全协作平台，定位信息安全从业者“瑞士军刀”，为用户提供安全大数据信息及高级工具等。使用对象主要为白帽子、信息安全从业者、及企业用户。

如有任何意见和建议，欢迎通过如下方式与我们联系：

联系邮箱：support@nosec.org

客服电话： 400-650-2031