

钓鱼产业

探索之道

cnsolu
data:04/17/2016



whoami



cnsolu

小鲜肉

Whitecell-club成员

白帽子

Weibo:<http://www.weibo.com/cnsolu>

Mail:cnsolu@whitecell-club.com



细数那些钓鱼站点

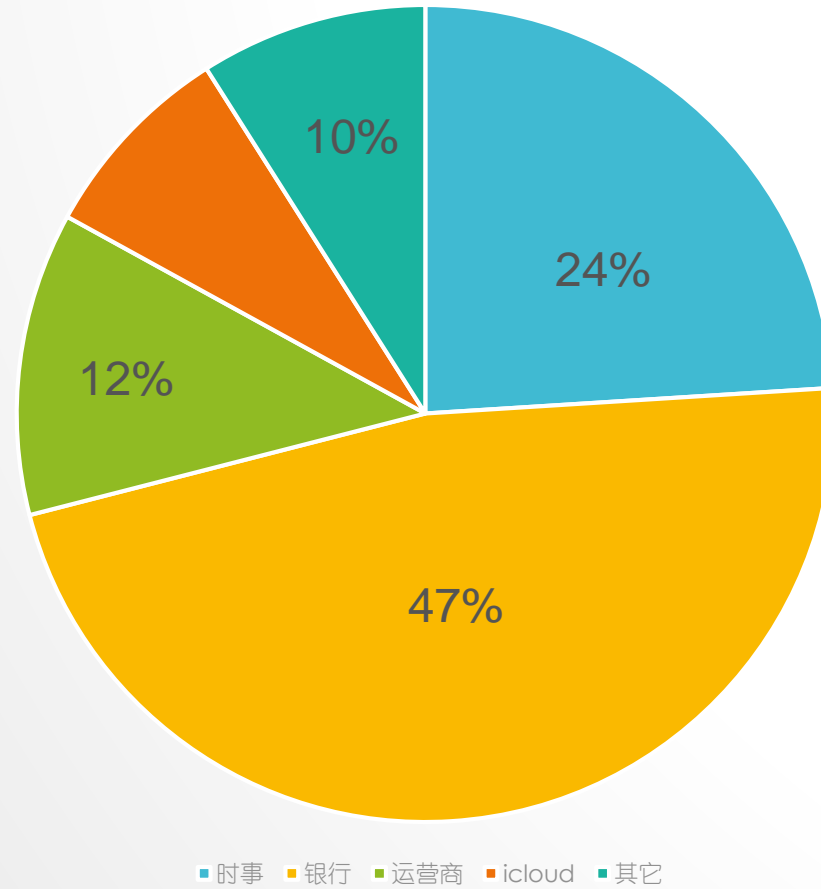


wap.10086.com
wup.10086.com
www.10086.com
www.10086-pp.com
wap.10086.cc
m.10086p.com
10086huodong.com

app1e-icloud-ios.com
apple-china-icloud.com
apple-icoloid.com
apple-iforgot-appleios.com
apple-ioclod.com
apple-iu-kefu.com
apple-iz-shouhou.com
appleis-iphone.com
applelp.com
appstore5.com



钓鱼站点类型统计





猫池



邮件传播





尊敬的用户您好

恭喜您！你的手机号码已被浙江卫视『奔跑吧兄弟』第三季抽选为二等奖幸运用户：活动将为您提供梦想创业基金¥100000元与苹果MacBook Pro笔记本电脑一台。请点击进入 syhui.com 查收领取！你的随机码【6568】请及时办理领奖手续。注：本次活动已通过互联网公证审批，请在限定时间内领取！如将个人领奖信息泄露给他人造成冒名领取本台概不负责！

尊敬的客户，你在我行账户积分已满一万分，可兑换500元现金礼包，请登陆 www.gsicku.com 查询兑换，逾期清零【工商银行】



亲：商一城后台评你为淘用户。我们已为你奉上¥160000和电脑一个。详：zxxm49.com 数字签入 8998

尊敬的建行用户：您账户已满50000积分可兑换5%的现金，请登录手机网 wap.desxa.cc 查询兑换，逾期失效【建设银行】

尊敬的客户您好！根据您的综合评分，现可提升50%固定额度，如需办理，请点击《wap.tr508.com/cn》在线申请【广发银行】

尊敬的用户：我行将开展个人信息核实认证，请登陆 wap.lczda.com 按提示核实，未核实账户将于今日24点冻结【工商银行】



iCloud 设置说明 | ?

登录 iCloud

11:01 PM 50

j10086hfg.com 15

中国移动 China Mobile 掌上营业厅 wap.10086.cn

首页 充值 查询 办理 优惠

您可用积分: **31600 分**
您可以兑换: **¥316.00 元人民币**
现在就去兑换

业务查询

账单查询	余额查询
GPRS流量查询	积分查询
在用业务查询	归属地查询

业务办理

【套餐】
全球通统一资费套餐
随e行无线宽带(WLAN)

【生活?娱乐】
139邮箱 飞信
号簿管家 彩铃

10:57 PM 14

m.cbusx.com/login.asp?id=3

中国银行 BANK OF CHINA

网银登录
用户名
密 码
附 加 码 462
记住用户名

下 一 步

10:49 PM 45

benss.cc/RunnerM/Home/Index 14

干大事,兄弟一起上!
特别惊喜

《奔跑吧兄弟》栏目开播以来收到全国观众的长期观看与热爱,同时为了答谢全国观众的大力支持,“奔跑吧兄弟”栏目在本月联合苹果中国商城举办活动全国手机用户抽奖活动。面向全国的手机用户抽选场外幸运用户!我们会通过“浙江卫视-奔跑吧兄弟”栏目抽选平台面向全国所有手机号码抽选。只要您是手机用户就有机会被“奔跑吧兄弟”栏目抽中,我们会通过系统短信的方式通知用户,请收到短信的用户使用手机登录领取奖项!

请在下方输入获奖手机号及幸运码

手机号码:

验证码:

我要领奖



会员管理后台

欢迎您: (admin) | 退出后台

ID	帐号	密码	姓名	身份证	手机	CNV	有效期	金额	是否通过	操作	次数	验证码	系统	在线	时间	操作
753	6212263400016460908	960610	张浩	371312199606105737	15140515561			0	未通过	未通过	1		苹果	在线	21:49	删除
752	6217213400011034609	180728	江慧	210213198207186024	15840937319			0	通过	未通过	1		苹果	离线	21:42	删除
750	6222023400012538426	611113	刘健	210211196111130411	13840841577			0	通过	未通过	0		苹果	离线	21:25	删除
749	6222023400018058965	100859	林功惠	210204196209146215	13709868376			5000	通过	未通过	0		苹果	离线	21:15	删除
748	6212813400000554943	121314	任洪旭	232302199610204110	13504089822			0	此银行卡积	未通过	0		苹果	离线	21:10	删除
747	6222310079235562	831219	吕雪松	210213198312196021	13478500750			4975	通过	未通过	1		苹果	离线	21:5	删除
746	62122263400016934365	890816	刘丹	210283199010192248	15242654989			0	通过	未通过	1		安卓	离线	21:3	删除
745	6215583400000731823	199410	尹传昊	210213199410043015	13234051090			0	通过	未通过	1		安卓	离线	21:0	删除
744	6212813400000554943	121314	任洪旭	232302199610204110	13504089822			0	此银行卡积	未通过	0		苹果	离线	20:58	删除
743	6212813400000554943	121314	任洪旭	232302199610204110	13504089822			0	此银行卡积	未通过	0		苹果	离线	20:53	删除
742	6222310082170160	110500	于永成	210213198810306010	18342045556			46	通过	未通过	1		苹果	离线	20:44	删除

紫缘网络安全测试系统

繁體語言

管理首頁

提交

記錄編號:331

APPLE ID : QQ號碼 : 986727874.qq.com(apple)

APPLE密碼 : QQ密碼 : Xin9521520

出生日期 : 1994, 10, 11

密保問題 : 你在学生时代最喜欢哪个歌手或乐队? , 魏晨 你的第一个宠物叫什么名字? , 大宝 你购买的第一张专辑是什么? , 千方百计

操作系統 : iPhone IOS

瀏覽器類型 : Safari瀏覽器

IP地址 : 117.136.5.82 【封鎖此IP地址】

使用代理 : 否

入口地址 : 27.126.188.30

加入時間 : 2016-3-31 12:16:44

刪除數據

刪除數據并拒收此資料

- 封鎖IP地址
- 資料黑名單
- 操作日誌
- 回收站
- 短信平台

記錄編號:335

APPLE ID : QQ號碼 : 1239095227@qq.com(apple)

APPLE密碼 : QQ密碼 : Dms051494

出生日期 : 1994, 09, 4

密保問題 : 你小时候最喜欢哪一本书? , 符仲 你的第一个上司叫什么名字? , 符仲 你上小学时最喜欢的老师姓什么? , 符仲

操作系統 : iPhone IOS

瀏覽器類型 : Safari瀏覽器

IP地址 : 1.192.158.83 【封鎖此IP地址】

使用代理 : 否



哪些人容易受骗？

哪些地区的人容易受骗？

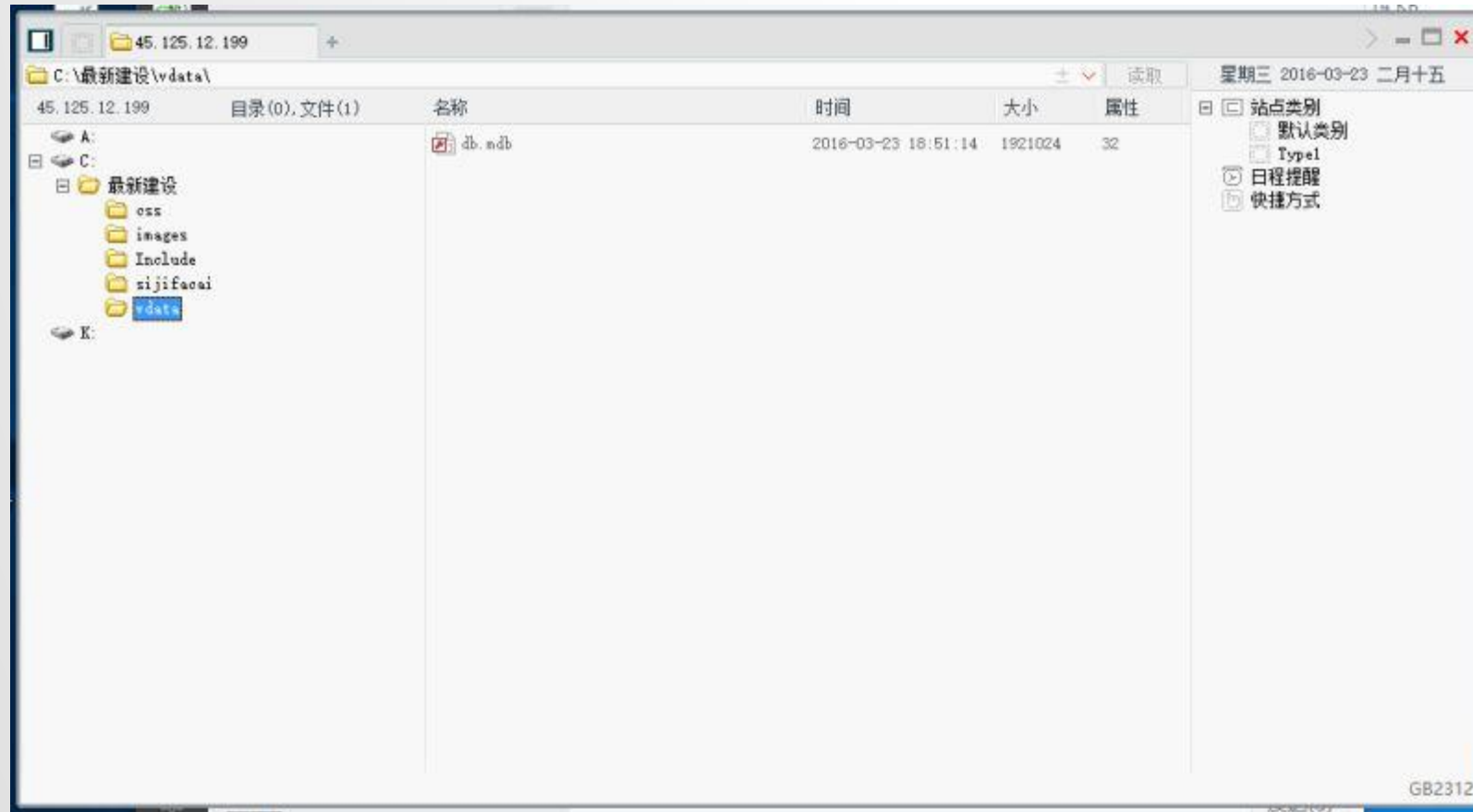
平均每个账户的损失是多少？



年轻人受众远远大于老年人
人群主要分布在监管不严的二、三线城市
平均每个账户损失金额在500~1500元不等



我要反击了!!!



80%以上都是ASP程序

存在漏洞：

XSS

sql-inject

越权

默认数据库下载

backdoor





我们应该怎么去做？



- 1.练就一双火眼，巧识真假网站
- 2.面对诱惑，静下心来想想
- 3.敏感信息三思后再考虑是否填写



臣妾做不到！



安全路，任重而道远



THX