互联网金融行业安全值报告

（2016 第一季度）

www.aqzhi.com

2016.5

报告概述

安全值行业报告是基于威胁情报数据，利用大数据的分析方法对行业整体安全状态进行评价和分析，本报告对互联网金融行业中 336 家互联网金融公司进行安全评价和量化风险分析。

本报告是针对各互联网金融公司的数据信息进行采集，共计 336 家公司的安全值进行分析，包括第三方支付 44 家、P2P 公司 150 家、众筹 110 家、消费金融 32 家，并从业务安全、隐私安全、应用安全、主机安全、网络安全、环境安全 6 个维度进行风险量化分析。

通过安全值对行业第一季度的数据分析发现：

根据 2016-5-4 安全值数据，互联网金融行业安全值为 857，整体评价为“一般”。共 336 个公司，其中 **182 家（54%）评价为“良好”；99 家（30%）评价为“一般”；55 家（16%）评价为“较差”**。

隐私安全问题较为普遍，336 家机构中 288 家存在该风险，约 86%，主要是域名未进行隐私保护问题较多，属于影响范围大，但影响程度一般的情况，**336 家机构中有 288 家（86%）的域名未做隐私保护，存在域名信息泄露风险，构成了隐私安全的主要问题。1097 个域名没有申请域名隐私保护，通过 Whois 可以查询域名注册信息。**

其次是应用安全和网络安全问题，在 336 家中有 140 家存在应用安全风险，约占 42%，主要问题是第三方漏洞平台上被发布安全漏洞和经常受到 Web 攻击，其中**有 134 家机构（40%）被公开披露了安全漏洞，构成了应用安全威胁的主要问题。近 90 天内共发现 208 条第三方安全社区上的安全漏洞记录，平均每个公司 30 天内被披露 1.5 个漏洞。**

336 家机构中有 111 家（33%）公司存在僵尸网络的风险，**90 天内共有 55 个 IP 网络受到影响，共发现 2381 条对外的非法攻击请求。**

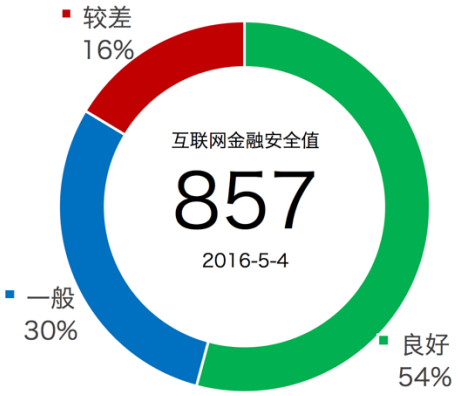
风险指标说明

安全值根据外部大数据和威胁情报数据进行挖掘，建立并持续更新指标体系，当前由 12 项安全风险指标支撑安全评价和分析。

- 域名劫持　域名解析异常，部分用户数据可能被非法劫持。
- 域名被封　域名被判定为不可信任的域名，部分用户可能无法访问
- 邮箱被封　邮件地址被认为垃圾邮件域，发出的邮件可能被认为垃圾邮件
- IP 被封　IP 被判定为恶意地址，可能影响网络正常通讯
- 漏洞披露　在互联网安全社区上披露了系统的安全漏洞
- Web 攻击　在线 Web 系统遭受了黑客的 Web 攻击或扫描
- 域名信息泄露　域名未做隐私保护，域名管理员可能会遭受钓鱼攻击
- 帐号信息泄露　企业的员工帐号在第三方数据库中被泄露，可能包括密码等敏感信息
- 恶意代码　信息系统上发现后门、病毒、木马等恶意代码
- 僵尸网络　网络内的主机可能已经被入侵，并植入木马、后门程序
- 异常流量　在线系统或网络遭受 DDOS 拒绝服务攻击
- 公有云风险　您正在与恶意网站共用同一个云服务资源

目录

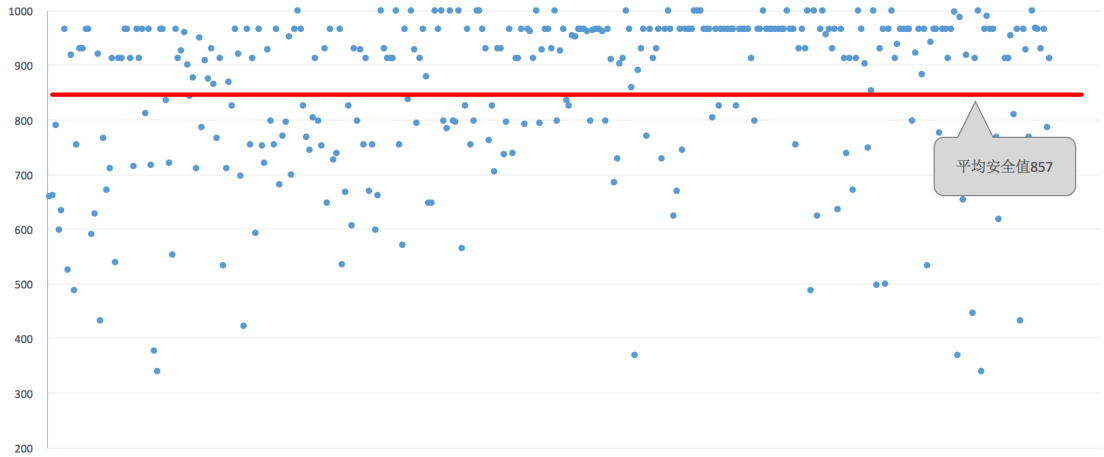
1. 行业总体概况



根据 2016-5-4 安全值数据，互联网金融行业安全值为 857，整体评价为 “一般”。共 336 个公司，其中 182 家（54%）评价为“良好”；99 家（30%）评价为“一般”；55 家（16%）评价为“较差”。

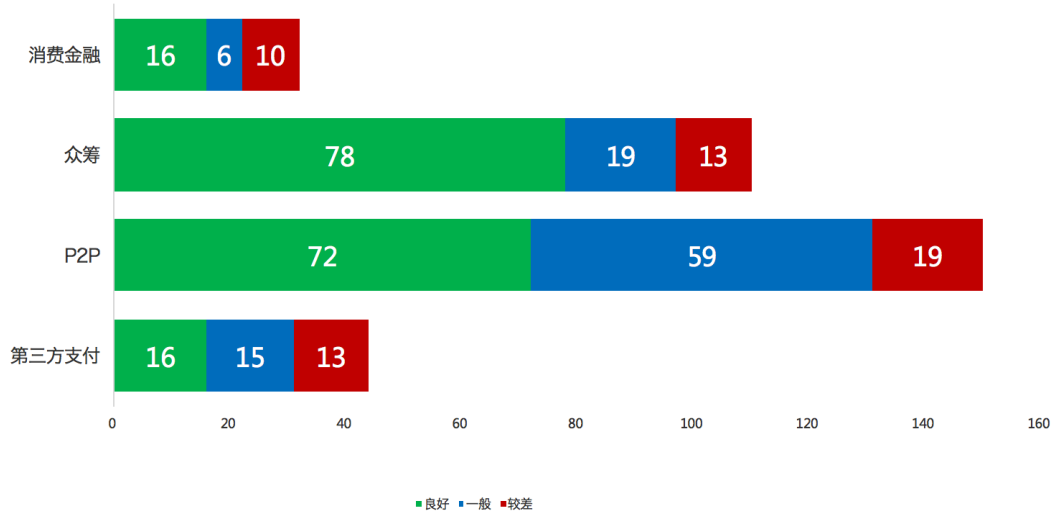
评价	得分范围	单位数量	占比
良好	901-1000	182	54%
一般	601-900	99	30%
较差	400-600	55	16%

1.1. 总体安全值分布



从安全值的分布情况来看，其中 211 家机构得分高于或等于平均值 857，125 家机构得分低于平均值，安全值得分分布大多数集中在良好的状态，平均分数线主要被过低的得分公司影响，最低分数为 339 分。

1.2. 按照业务分类统计



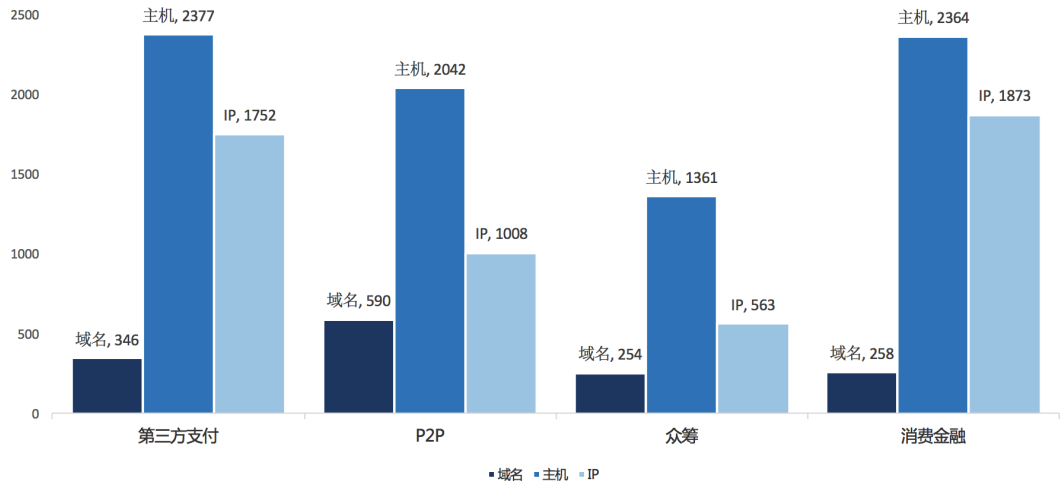
	平均值	机构数量	良好	一般	较差
第三方支付	780	44	16	15	13
P2P	853	150	72	59	19
众筹	902	110	78	19	13
消费金融	829	32	16	6	10

根据业务类型分类，P2P 公司数量最多，150 家机构中“一般”和“较差”水平的有 78 家，占城商行的 52%，平均安全值为 853 分；

众筹公司的平均安全值最高 902 分，110 家机构中“一般”和“较差”水平的有 32 家，仅占众筹公司的 29%。

1.3. 互联网资产统计

安全值对互联网资产进行分析统计，包括各机构注册的域名、面向互联网开放的主机服务（不仅限于 Web 服务的网站）和公网 IP 地址。

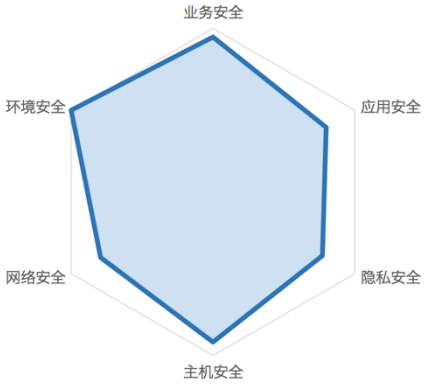


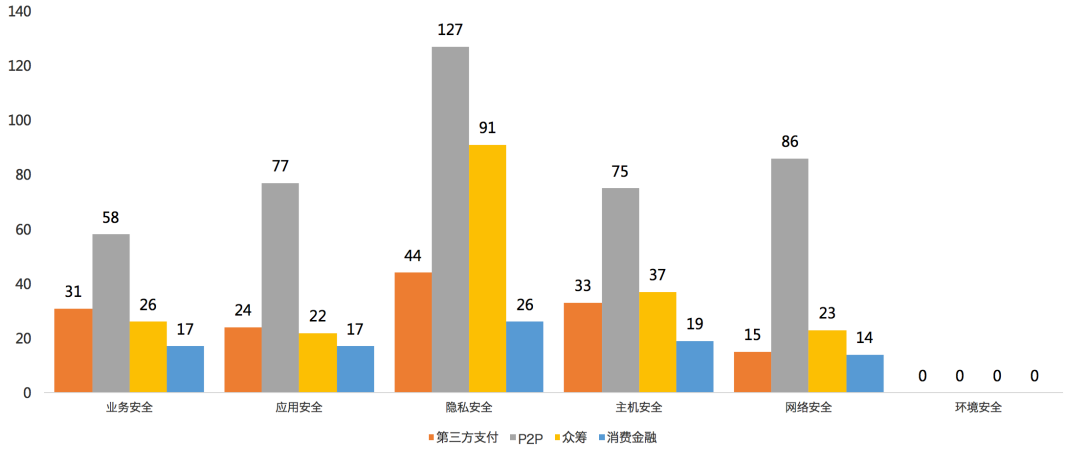
	域名数量	主机数量	IP 数量	平均每机构资产数量
第三方支付	346	2377	1752	102
P2P	590	2042	1008	24
众筹	254	1361	563	20
消费金融	258	2364	1873	140
总体	1448	8144	5196	44

44 家第三方支付公司的资产数量较多，同时面临的风险最大，根据对互联网开放的域名、主机和 IP 地址统计，第三方支付公司域名共有 346 个，公网主机 2377 个，公网 IP 地址 1752 个，平均每个机构有 102 个互联网资产，安全值平均得分 780。

2. 风险分布及量化评估

根据业内的信息安全风险管理最佳实践，结合风险等级、影响范围、频率、数量、时间各方面要素建立量化风险的计算模型，对整体情况的 6 个风险域（业务安全、应用安全、隐私安全、主机安全、网络安全和环境安全）进行量化评价，综合来看隐私安全问题普遍存在，其次是应用安全和网络安全方面。





	机构数量	业务安全	应用安全	隐私安全	主机安全	网络安全	环境安全
第三方支付	44	31	24	44	33	15	0
P2P	150	58	77	127	75	86	0
众筹	110	26	22	91	37	23	0
消费金融	32	17	17	26	19	14	0
总计	336	132	140	288	164	138	0

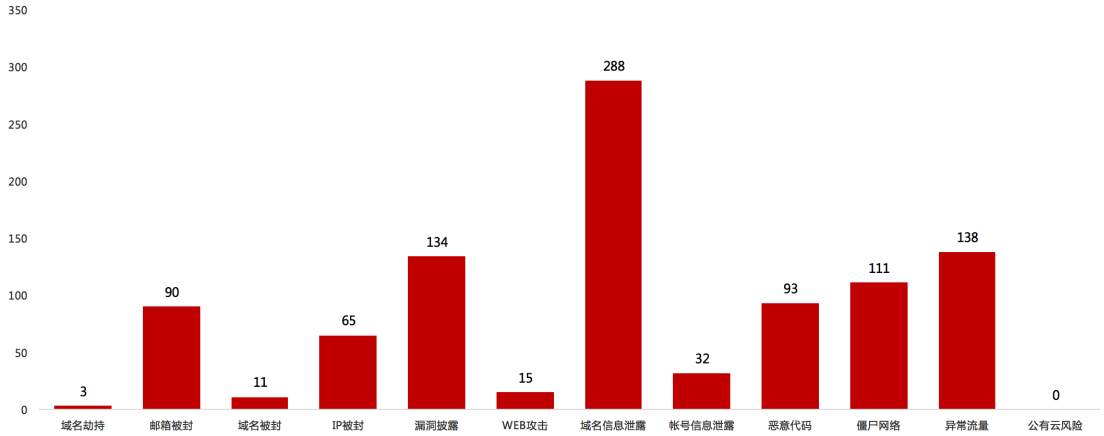
通过安全值对互联网金融行业第一季度的数据分析发现：

1. 隐私安全问题较为普遍，336 家机构中 288 家存在该风险，约 86%，主要是域名未进行隐私保护问题较多，该风险影响范围大，但影响程度一般，风险详细分析见 3.3 章。
2. 其次是应用安全和主机安全问题，在 336 家中有 140 家存在应用安全风险，约占 42%，主要问题是第三方漏洞平台上被发布安全漏洞，336 家机构中有 111 家（33%）

公司存在僵尸网络的风险，风险详情见 3.1 章和 3.2 章。

3. 主要风险详细分析

安全值整体基于 12 个风险指标支撑 6 个维度的安全评价，分别对各项风险指标影响的机构数量进行统计便于找出较集中的问题。

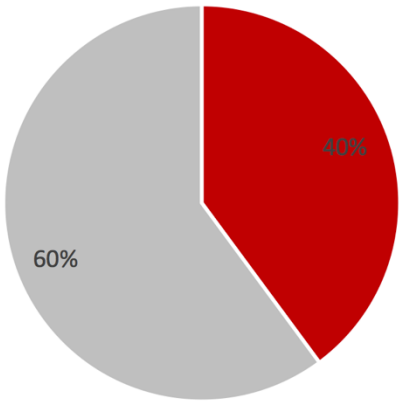


	域名劫持	邮箱被封	域名被封	IP被封	漏洞披露	WEB攻击	域名信息泄露	帐号信息泄露	恶意代码	僵尸网络	异常流量	公有云风险
第三方支付	0	28	5	12	24	1	44	20	29	19	15	0
P2P	2	37	3	27	75	6	127	8	39	50	86	0
众筹	0	10	1	18	18	5	91	1	10	31	23	0
消费金融	1	15	2	8	17	3	26	3	15	11	14	0
总体	**3**	**90**	**11**	**65**	**134**	**15**	**288**	**32**	**93**	**111**	**138**	**0**

3.1. 漏洞披露风险分析

互联网安全社区上公开披露的安全漏洞应该优先处理，避免漏洞在修复之前被公开，引来恶意攻击和影响形象，应通过安全顾问的帮助分析问题的根源，避免同类漏洞的产生。

漏洞披露



336 家中有 134 家机构（40%）被公开披露了安全漏洞，构成了应用安全威胁的主要问题。

近 90 天内共发现 208 条第三方安全社区上的安全漏洞记录，平均每个公司 30 天内被披露 1.5 个漏洞。

[redacted]	处设计缺陷可刷单	2016-05-03
[redacted]	工邮箱弱口令泄露未来技术规划涉及用户手	2016-05-03
[redacted]	简单单通用存储型xss	2016-05-03
[redacted]	某系统tomcat配置不当可getshell	2016-04-29
[redacted]	app几种安全问题	2016-04-28
[redacted]	Android客户端远程命令执行	2016-04-28
[redacted]	器远程命令执行漏洞	2016-04-28
[redacted]	某站SQL注射漏洞	2016-04-28
[redacted]	某站配置不当导致getshell可威胁内网	2016-04-28
[redacted]	某重要系统任意密码重置	2016-04-28
[redacted]	统存在SQL注入	2016-04-27
[redacted]	漏洞泄露敏感信息(cookie\电话\名字\身份证	2016-04-27
[redacted]	多处注入	2016-04-27
[redacted]	多处注入	2016-04-27
[redacted]	的xss	2016-04-27

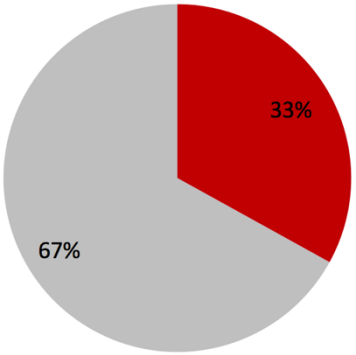
处置建议：

1. 及时与第三方漏洞平台取得联系，认领安全漏洞，并进行漏洞修补；
2. 对漏洞修补后的效果进行验证；
3. 对所有系统全面进行安全漏洞检查和渗透测试，对漏洞进行分类管理，跟踪漏洞处置过程和结果，完善上线安全测试工作，保证信息系统无高、中危的安全漏洞。

3.2. 僵尸网络风险分析

网络内的服务器或者终端已经被植入木马、后门，被非法控制成为“肉鸡”，对外发起了扫描或者攻击的行为。

僵尸网络



336 家机构中有 111 家（33%）公司存在僵尸网络的风险。

90 天内共有 55 个 IP 网络受到影响，共发现 2381 条对外的非法攻击请求。

公司	2 .124	2016-05-03 13:29:47	ab.w ss.com	tcp@syn_flood_source	3879
公司	2 .98.2 .124	2016-05-03 13:24:42	ab.w w.5 ss.com	tcp@syn_flood_source	3246
公司	2 .98.2 .124	2016-05-03 13:04:46	ab.w w.5 ss.com	tcp@syn_flood_source	442
公司	2 .98.2 .124	2016-05-03 10:54:56	ab.w w.5 ss.com	tcp@syn_flood_source	1073
子支付服务有限公司	1 .59.2 .120	2016-05-03 00:00:00		C&C;	IP used by suppobox C&C+
子支付服务有限公司	1 .59.2 .120	2016-05-03 00:00:00			
	6 172.2 .153	2016-05-03 00:00:00		C&C;	IP used by suppobox C&C+
算	4 120.1 .78	2016-05-03 00:00:00			
家	1 .24.8 .217	2016-05-03 00:00:00			Scanning Host+:[;
	4 120.1 .78	2016-05-03 00:00:00			
使	4 120.1 .78	2016-05-03 00:00:00			
公司	1 .247. .105	2016-05-03 00:00:00			
公司	1 .247. .97	2016-05-03 00:00:00			
公司	1 .247. .100	2016-05-03 00:00:00			
公司	2 .98.2 .124	2016-05-02 10:07:11	ab.w w.5 ss.com	tcp@syn_flood_source	1918
子支付服务有限公司	1 .59.2 .120	2016-05-02 00:00:00		C&C;	IP used by suppobox C&C+
子支付服务有限公司	1 .59.2 .120	2016-05-02 00:00:00			
	6 172.2 .153	2016-05-02 00:00:00		C&C;	IP used by suppobox C&C+
算	4 120.1 .78	2016-05-02 00:00:00			
家	1 .24.8 .217	2016-05-02 00:00:00			Scanning Host+:[;
	4 120.1 .78	2016-05-02 00:00:00			
东	1 .13.2 .10	2016-05-02 00:00:00			
使	4 120.1 .78	2016-05-02 00:00:00			
东	1 .13.2 .10	2016-05-02 00:00:00			
公司	1 .247. .105	2016-05-02 00:00:00			
公司	2 .98.2 .124	2016-05-01 18:59:33	ab.h 67. m	tcp@syn_flood_source	5182
公司	2 .98.2 .124	2016-05-01 13:20:45	ab.w w.5 ss.com	tcp@syn_flood_source	2298
	1 .188. .37	2016-05-01 10:56:16	www 24 net	[GET]Infomation Leak Attack	/template/.bashrc
公司	2 .98.2 .124	2016-05-01 01:29:38	ab.n .dn 3.com	tcp@syn_flood_source	6054
公司	2 .98.2 .124	2016-05-01 01:23:05	ab.n 3.com	tcp@syn_flood_source	7264
子支付服务有限公司	1 .59.2 .120	2016-05-01 00:00:00		C&C;	IP used by suppobox C&C+

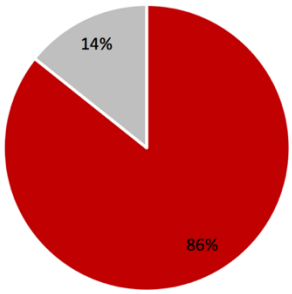
处置建议：

1. 分析僵尸网络地址对应网络，如果是服务器网络则需要对系统进行全面的风险评估；
2. 如果僵尸网络地址对应办公网，需通过出口路由器日志定位终端主机，并检查木马、后门，加强终端安全保护；
3. 加强终端使用安全管理，上网行为管理。

3.3. 域名信息泄露风险分析

在注册商成功注册域名后，你的姓名、联系地址、电话、Email 等注册信息将被存储到域名 whois 信息数据库中，任何人都可公开查询到这些信息，隐私无法保障。

域名信息泄露



336 家机构中有 288 家（86%）的域名未做隐私保护，存在域名信息泄露风险，构成了隐私安全的主要问题。

1097 个域名没有申请域名隐私保护，通过 Whois 可以查询域名注册信息。

[redacted]com	[redacted]com	phone	+85[redacted]
[redacted].com	[redacted]com	fax	+85[redacted]200
[redacted].com.cn	[redacted]com	email	dns[redacted]hk.alib[redacted]a-inc.com
[redacted].com.cn	[redacted].com	phone	+86[redacted]665588
[redacted].net	[redacted].com	email	yue[redacted]@zihex[redacted].com
[redacted].cn	[redacted].com.cn	email	cnn[redacted]adns.c[redacted]m
[redacted].net.cn	[redacted].com.cn	email	yue[redacted].com

处置建议：

与域名服务商联系，申请域名隐私保护。（域名隐私保护：指域名持有者可以通过自主设置保护域名注册人、电话、邮箱等信息不被公开，减少垃圾邮件、短信以及防止个人真实信息被窃取等。）

附表：互联网金融公司名单

字母排序，不分先后

北京拉卡拉网络技术有限公司	第三方支付
北京数字王府井科技有限公司	第三方支付
北京通融通信息技术有限公司	第三方支付
北京银联商务有限公司	第三方支付
渤海易生商务服务有限公司	第三方支付
东方电子支付有限公司	第三方支付
广州银联网络支付有限公司	第三方支付
海南海岛一卡通支付网络有限公司	第三方支付
海南新生信息技术有限公司	第三方支付
河北一卡通电子支付服务有限公司	第三方支付
江苏瑞祥商务有限公司	第三方支付
捷付睿通股份有限公司	第三方支付

开联通网络技术服务有限公司	第三方支付
快钱支付清算信息有限公司	第三方支付
联动优势电子商务有限公司	第三方支付
联通支付有限公司	第三方支付
钱袋网（北京）信息技术有限公司	第三方支付
山东鲁商一卡通支付有限公司	第三方支付
杉德电子商务服务有限公司	第三方支付
上海畅购企业服务有限公司	第三方支付
上海得仕企业服务有限公司	第三方支付
上海付费通信息服务有限公司	第三方支付
上海富友金融网络技术有限公司	第三方支付
上海汇付数据服务有限公司	第三方支付
上海捷银信息技术有限公司	第三方支付
上海盛付通电子支付服务有限公司	第三方支付
上海银联电子支付服务有限公司	第三方支付
深圳市财付通科技有限公司	第三方支付
深圳市快付通金融网络科技服务有限公司	第三方支付
深圳市泰海网络科技服务有限公司	第三方支付
深圳市壹卡会科技服务有限公司	第三方支付
深圳银盛电子支付科技有限公司	第三方支付
天津城市一卡通有限公司	第三方支付
天翼电子商务有限公司	第三方支付
通联支付网络服务股份有限公司	第三方支付
网银在线（北京）科技有限公司	第三方支付
武汉市金源信企业服务信息系统有限公司	第三方支付
迅付信息科技有限公司	第三方支付
易通支付有限公司	第三方支付
银联商务有限公司	第三方支付
裕福网络科技有限公司	第三方支付
证联融通电子有限公司	第三方支付
支付宝（中国）网络技术有限公司	第三方支付
资和信电子支付有限公司	第三方支付
168 理财网	P2P
365 易贷	P2P
91 旺财	P2P
e 路同心	P2P
E 速贷	P2P
PPmoney	P2P
爱钱帮	P2P
爱钱进	P2P
爱投资	P2P
安心 de 利	P2P
安心贷	P2P

安星财富网	P2P
抱财网	P2P
博金贷	P2P
财富中国	P2P
超人贷	P2P
诚汇通	P2P
城城理财	P2P
橙旗贷	P2P
大丰收金融	P2P
德众金融	P2P
地标金融	P2P
点融网	P2P
鼎信贷	P2P
短融网	P2P
付融宝	P2P
富春贷	P2P
共信赢	P2P
冠 e 通	P2P
广信贷	P2P
汉金所	P2P
好贷宝	P2P
合力贷	P2P
合拍在线	P2P
合盘贷	P2P
合时代	P2P
和信贷	P2P
恒信易贷	P2P
红岭创投	P2P
后河财富	P2P
互利网龙宝宝	P2P
互融宝	P2P
华融道	P2P
汇通易贷	P2P
汇投资	P2P
汇盈金服	P2P
积木盒子	P2P
集利财富网	P2P
金 e 贷	P2P
金宝保	P2P
金海贷	P2P
金控网贷	P2P
金联储	P2P
金粮宝	P2P

金牛在线	P2P
金票通	P2P
金融工场	P2P
金信网	P2P
金银猫	P2P
晋商贷	P2P
九斗鱼	P2P
钜宝盆	P2P
君融贷	P2P
开鑫贷	P2P
可溯贷	P2P
孔方兄	P2P
口贷网	P2P
懒投资	P2P
礼德财富	P2P
理财范	P2P
理想宝	P2P
力帆善融	P2P
连资贷	P2P
两只老虎	P2P
隆金宝	P2P
陆金所	P2P
绿化贷	P2P
美利金融	P2P
迷你贷	P2P
民信贷	P2P
你我贷	P2P
诺诺镑客	P2P
拍拍贷	P2P
普惠理财	P2P
普天贷	P2P
启道金融	P2P
千壹理财	P2P
钱爸爸	P2P
钱吧	P2P
钱多多	P2P
钱来网	P2P
趣钱	P2P
人人贷	P2P
人人聚财	P2P
人文贷	P2P
融贝网	P2P
融金所	P2P

融资易	P2P
瑞银创投	P2P
三信贷	P2P
杉易贷	P2P
商富贷	P2P
生菜金融	P2P
石投金融	P2P
首 E 家	P2P
四达投资	P2P
糖果金融	P2P
腾邦创投	P2P
投米网	P2P
投哪网	P2P
团贷网	P2P
拓道金服	P2P
网利宝	P2P
微贷网	P2P
温商贷	P2P
温州贷	P2P
沃时贷	P2P
向上金服	P2P
小微金融	P2P
小赢理财	P2P
小油菜	P2P
新联在线	P2P
新新贷	P2P
鑫合汇	P2P
信融财富	P2P
信用宝	P2P
雪山贷	P2P
迅泊达	P2P
一点通	P2P
宜人贷	P2P
易贷网	P2P
翼龙贷	P2P
银巴克	P2P
银豆网	P2P
银湖网	P2P
银客网	P2P
银票网	P2P
永利宝	P2P
有利网	P2P
有融网	P2P

粤商贷	P2P
长久贷	P2P
招商贷	P2P
浙商 E 贷	P2P
中广核富盈	P2P
中融宝	P2P
中瑞财富	P2P
众金在线	P2P
众信金融	P2P
珠宝贷	P2P
28 众筹	众筹
36 氪	众筹
58 众筹网	众筹
91 众筹	众筹
E 分投	众筹
e 人筹	众筹
V2IPO 创客	众筹
爱创业	众筹
爱就投	众筹
爱投社	众筹
百筹汇	众筹
北大创业众筹	众筹
本地众筹	众筹
伯乐合投	众筹
博点网	众筹
财富众投	众筹
车车车	众筹
筹道	众筹
筹趣网	众筹
触点众筹	众筹
创投圈	众筹
创投在线	众筹
创微网	众筹
创业 e 家	众筹
大伙投	众筹
大家筹	众筹
大家投	众筹
贷帮众筹	众筹
蛋芽网	众筹
第五创	众筹
东之贝	众筹
多彩投	众筹
蜂窝众筹	众筹

股筹网	众筹
股东汇	众筹
股权店	众筹
股众网	众筹
海鳖众筹	众筹
海力量	众筹
合伙圈	众筹
合伙中国	众筹
和云筹	众筹
黑马岛	众筹
汇梦公社	众筹
京北众筹	众筹
京东东家	众筹
九九众筹	众筹
聚合赢	众筹
聚募众筹	众筹
聚天下	众筹
开心投-	众筹
蝌蚪众筹	众筹
来筹网	众筹
乐耕	众筹
乐诸葛	众筹
领筹网/众筹所	众筹
牛投众筹	众筹
齐鲁众筹	众筹
麒麟众筹	众筹
汽车众筹	众筹
牵投	众筹
青桐树	众筹
全民众筹	众筹
人人合伙	众筹
人人投	众筹
陕众筹	众筹
天使汇	众筹
天使基金网	众筹
天使街	众筹
天使客	众筹
天使叔叔	众筹
天使营	众筹
天天投	众筹
同筹荟	众筹
投行圈	众筹
投壶网	众筹

投融界	众筹
微投网	众筹
文筹网	众筹
希望筹	众筹
香山众筹	众筹
小草众筹	众筹
协同工场	众筹
鑫筹所	众筹
星火投资	众筹
易筹网	众筹
益旺众筹	众筹
圆桌汇	众筹
源镕众筹	众筹
云岸金服	众筹
云筹	众筹
云研社	众筹
智金汇	众筹
智锐创想	众筹
中证众创	众筹
众筹邦	众筹
众筹界	众筹
众筹客	众筹
众创众筹	众筹
众家投	众筹
众投邦	众筹
众投客	众筹
众投社	众筹
众投天地	众筹
众源众筹	众筹
众众投	众筹
洲际联合	众筹
追梦网	众筹
资本汇	众筹
总裁汇	众筹
阿里花呗	消费金融
爱学贷	消费金融
百度有钱	消费金融
北银消费金融	消费金融
鼎力分期	消费金融
分期范	消费金融
分期管家	消费金融
分期乐	消费金融
付壹贷	消费金融

瓜牛分期	消费金融
国美消费金融	消费金融
海尔消费金融	消费金融
湖北消费金融	消费金融
捷分期	消费金融
捷信消费金融	消费金融
金融 1 号店	消费金融
金融猫	消费金融
锦程消费金融	消费金融
京东白条	消费金融
桔子分期	消费金融
马上消费金融	消费金融
名校贷	消费金融
平安消费金融	消费金融
人人分期	消费金融
苏宁消费金融	消费金融
天天分期	消费金融
万达消费金融	消费金融
先花花	消费金融
信通袋	消费金融
兴业消费金融	消费金融
优分期	消费金融
中银消费金融	消费金融