SACC 2014中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2014
发现架构之美

P2P行业风险分析与安全防御

网信金融 刘斐然

问题一：什么是P2P？

问题二：P2P借贷中会遇到哪些安全风险？

问题三：如何防御？

什么是P2P？

互联网金融

金融机构互联网 = 传统金融机构 + 互联网渠道

互联网企业金融 = 互联网行业 + 金融业务

互联网金融的几大模式

第三方支付平台模式

代表企业：支付宝、易宝支付、拉卡拉、财付通

互联网理财销售模式

代表产品： 余额宝

P2P网络信贷模式

所谓P2P，其实是Peer-to-Peer lending，即点对点信贷的简称，简单称为称个人对个人信贷，在央行的相关文件里，正式叫法为人人贷（并非特指人人贷公司，而是对当前所有P2P公司的一个总称）。

模式概述：通过P2P网络融资平台，借款人直接发布借款信息，出借人了解对方的身份信息、信用信息后，可以直接与借款人签署借贷合同，提供小额贷款，并能及时获知借款人的还款进度，获得投资回报。

核心逻辑：所谓P2P，模式的本质其实就是一个互联网平台通过网络一端对接有小额借款需求的人，一端对接有理财需求的人。拆成两半就是一个理财平台加上一个小额贷款平台。

代表企业：美国的prosper和lendingclubP2P公司，国内的人人贷、红岭创投等。

传统理财方式

特色：

1. 存款人/投资者与金融机构签约（属于债权关系）
2. 以金融机构的信誉为主要考量（融资方的资质不重要）
3. 通过金融机构提供的专业人士进行资金投放
4. 金融机构多数提供保本的低收益

P2P理财方式

投资者

直接对接

渠道、平台

融资方

中介机构

- 金融机构
- 担保公司
- 网站平台
- 咨询公司

特色：

1. 投资者直接与融资方签约
2. 融资方的资质与项目透明
3. 通过借贷方式获得收益，简单直接
4. 投资者所需金融相关专业知识要求高

众筹融资模式

模式概述：所谓众筹平台，是指创意人向公众募集小额资金或其他支持，再将创意实施结果反馈给出资人的平台。网站为网友提供发起筹资创意，整理出资人信息，公开创意实施结果的平台，以与筹资人分成为主要赢利模式。

核心逻辑：在互联网上通过大众来筹集新项目或开办企业的资金。

代表企业：国外最早和最知名的平台是kickstarter，国内有点名时间、众筹网、淘梦网等。

金融服务平台模式

虚拟电子货币模式

……

网信金融

一站式互联网金融综合服务商

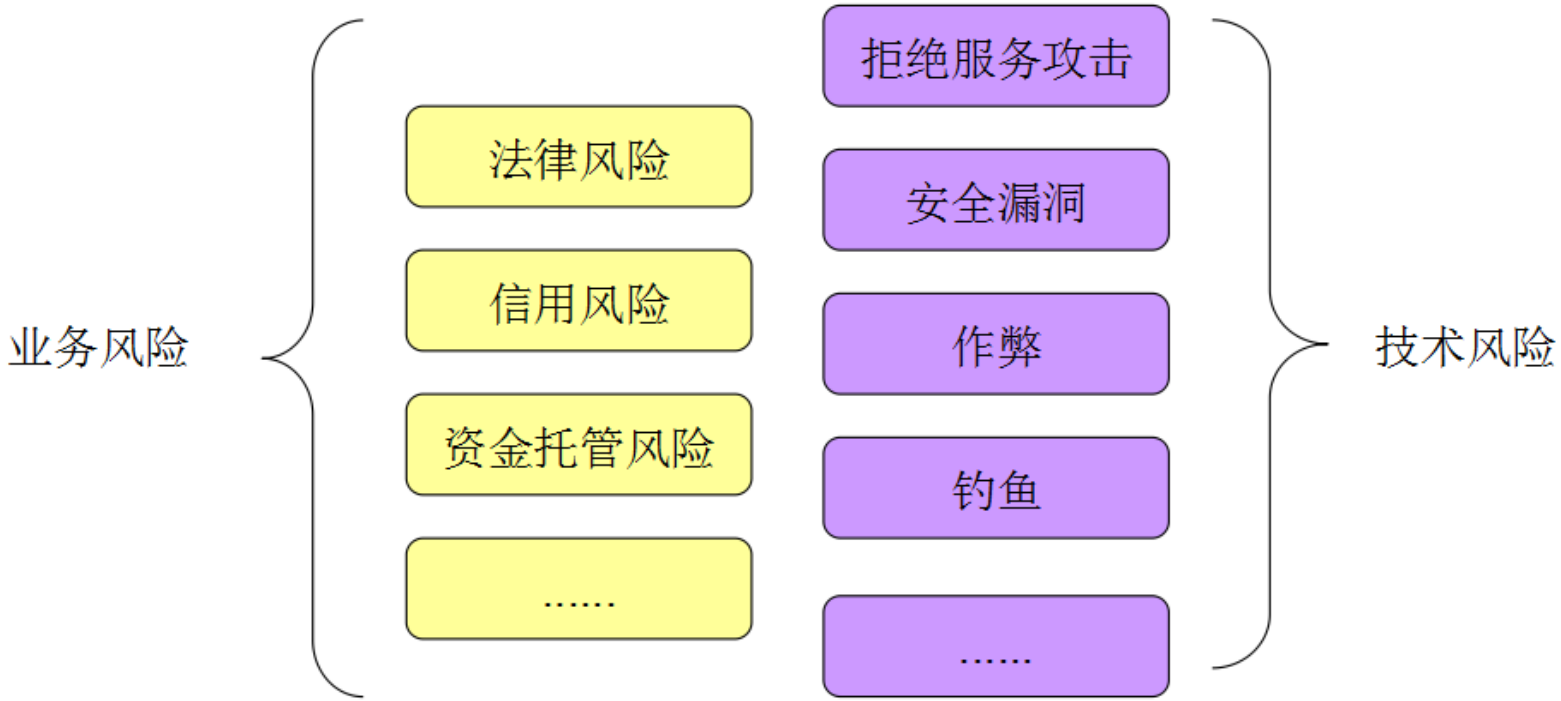
- 愿景：智慧金融创造美好人生
- 覆盖全国的经营网络和多牌照的服务平台
- 主营业务：网络融资（P2P贷款、众筹融资、电商小贷）、支付结算、金融产品电商网销、金融理财信息搜索与咨询
- 已建立华北、华中、华东、华南等四个区域总部

全部(2417) | 新手专享(468) | 产融贷(553) | 车贷(216) | 房贷(553) | 应收贷(276) | 典当贷(46) | 租上租(66) | 医疗贷(14) | 其它(225)

投资项目	年化收益率	期限	收益方式	投资进度	状态
房贷 18万一口标，乐居贷024 总额：18.00万	9.5%	6个月	按月付息到期还本	可投金额：180,000.00元 售前预约中	预约中
企业贷 100起投，长兴2号001-17 总额：100.00万	8.00%+1.50% APP专享	2个月	一次性还本付息	可投金额：943,244.65元 剩余时间：6天23时51分	投资
企业贷 100起投，长兴2号001-16 总额：100.00万	8.00%+1.00%	2个月	一次性还本付息	可投金额：986,657.18元 剩余时间：6天23时50分	投资
租上租 定额20，华赢1号008-28 总额：0.80万	8.30% APP新手大奖标	177天	一次性还本付息	可投金额：6,940.00元 剩余时间：6天23时32分	投资
企业贷 10万起投，长兴2号001-14 总额：200.00万	8.00%+2.00%	2个月	一次性还本付息	可投金额：1,299,922.48元 剩余时间：6天23时27分	投资
车贷 1万起投，车易盈162-4 总额：100.00万	9.50%+0.40%	6个月	按月付息到期还本	可投金额：561,088.81元 剩余时间：6天19时47分	投资

P2P借贷过程中会遇到哪些安全风险？

P2P行业风险



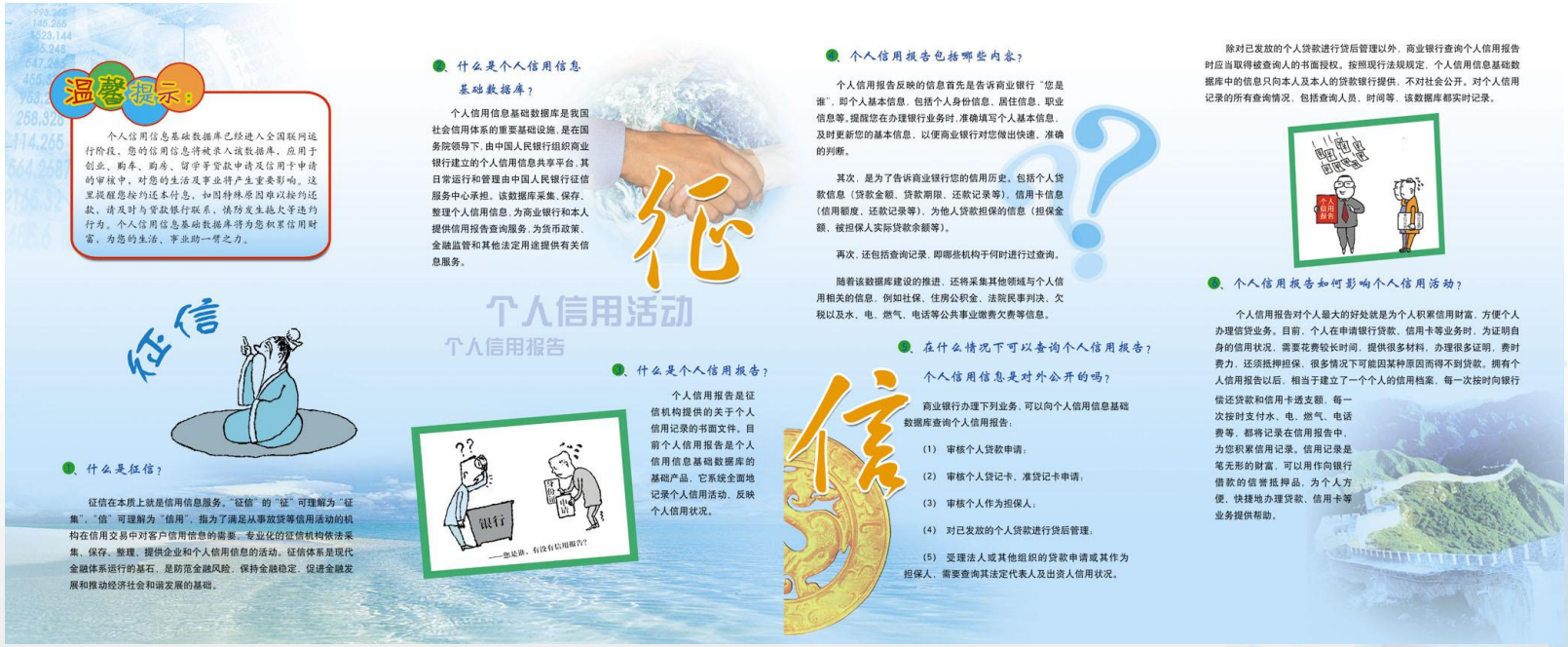
法律风险

- 法律制度不完善

- 央行定制的P2P业务经营红线
  - 本身不得提供担保
  - 不得归集资金搞资金池
  - 不得非法吸收公众存款
  - 不能实施集资诈骗

信用风险

- 借款人违约及虚假借款人是信用风险的两大主体



资金托管风险

- 第三方托管平台

  第三方资金托管是指资金流运行在第三方资金托管公司，而不经过平台账户。从而避免了平台恶意挪用交易资金给投资人带来的风险

- 常见手段
  - 有名无实
  - 鱼目混珠
  - 狐假虎威

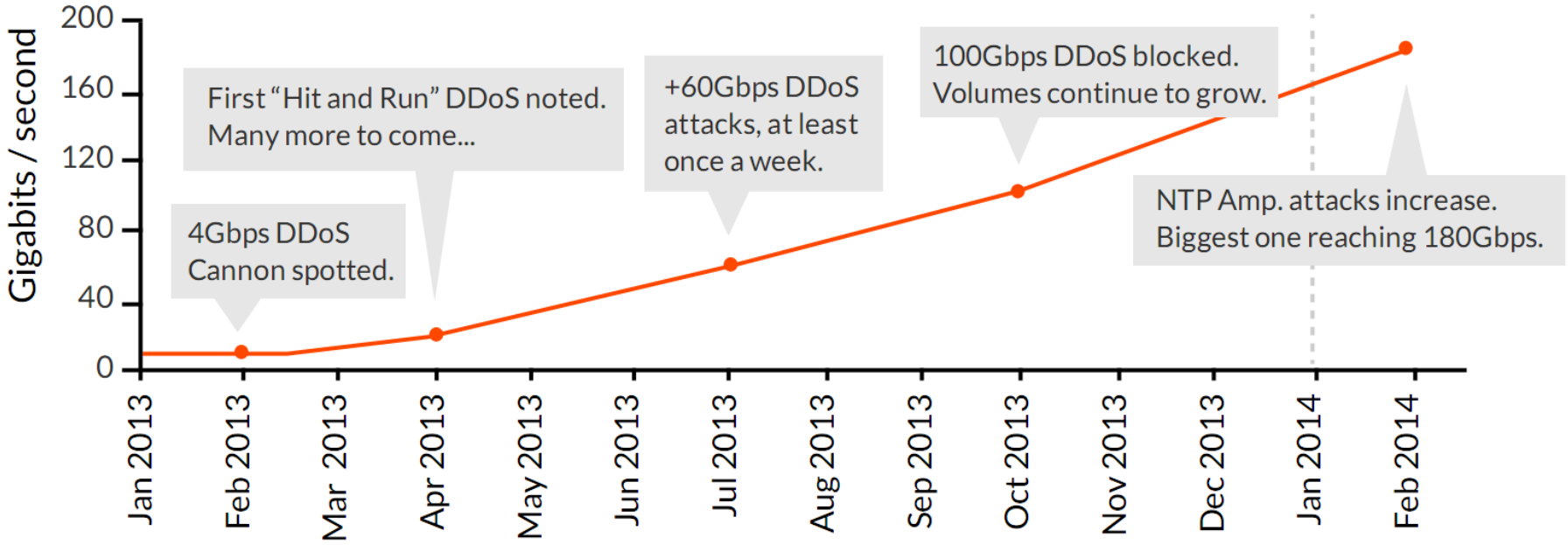
拒绝服务攻击


攻击者
正常HTTP Get Flood
正常HTTP Get Flood
正常HTTP Get Flood
正常HTTP Get Flood
正常HTTP Get Flood
正常HTTP Get Flood
受害者(Web Server)
不能建立正常的连接
正常用户

拒绝服务攻击

Network (Layers 3 & 4) DDoS Attacks

2013: Overview



拒绝服务攻击的方式

- 传统做法，针对带宽与
  SYN Flood/UDP Flood/ICMP Flood/CC ...

- 改进做法
  - 攻击服务：
    - nginx：CVE-2013-2070/ apache：CVE-2011-3192
  - 攻击协议：
    - SSL协议漏洞
  - DRDoS（分布式反射攻击）：可以获得几倍到几百倍的带宽放大
    - NTP 反射攻击
    - DNS 反射攻击
    - SNMP 反射攻击
    - 应用程序反射

拒绝服务攻击威胁

- 特点：
  - 实施攻击特别简单，工具完善。
  - 见效显著
  - 任何网站均有被拒绝服务攻击的潜在风险

- 造成后果：
  - 服务器停止响应
  - 用户流失
  - 平台倒闭

安全漏洞

- 操作系统漏洞/底层服务漏洞/协议漏洞
- WEB应用安全漏洞
  - SQL注入
  - XSS/CSRF
  - 平行权限
  - 业务逻辑漏洞
  - 包含脆弱的开源系统
  - ……

例1: 形同虚设的支付密码

- 某网站设置了用户登录密码，支付密码。

例2: 暴力登录

- 用户密码泄露

例2: 暴力登录

- 无验证码或验证码过于简陋







例3: 平行权限

如果一个提供用户资料的页面,未做资源授权限制:

www.xxx.com/user?id=1 或 www.xxx.com/user/info/1

则遍历ID即可便利此网站的用户

Insecure Direct Object References

安全漏洞威胁

- 特点：
  - 实施攻击简单，工具完善。
  - 见效显著
  - P2P行业中存在大量WEB应用层安全漏洞

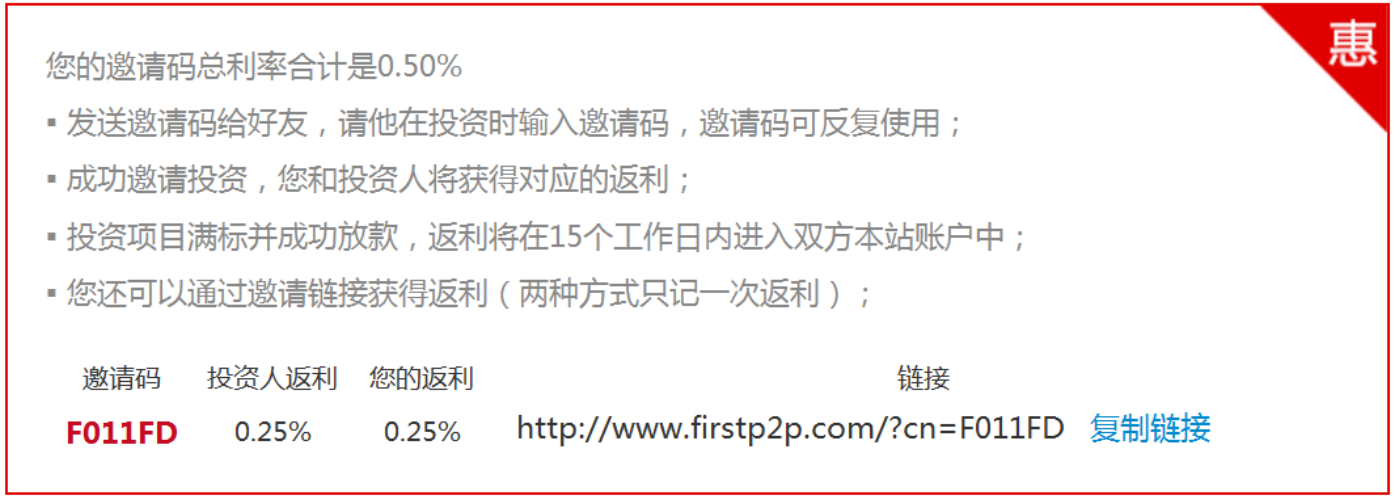
- 造成后果：
  - 机密数据，客户资料丢失
  - 关键数据被修改
  - 服务器沦陷

作弊

- 个人活动作弊
  - 身份证信息泄露
  - 产业链完善

作弊

- 流量劫持
  - DNS劫持
  - 小区宽带劫持
  - 无线网络劫持
  - ……



作弊威胁

- 特点：
  - 攻击者可以获得直接利益
  - 作弊工具自动化
  - P2P行业大量的返现活动成为其目标
- 造成后果：
  - 公司遭受经济上的损失

钓鱼


中国银行全球门户网站 - Windows Internet Explorer
http://www.bocws.tk/
域名高度近似的"钓鱼"网址
中国银行全球门户网站
中国银行全球门户网站 - Windows Internet Explorer
http://www.boc.cn/
中国银行官方网站地址
中国银行全球门户网站
中国银行
BANK OF CHINA
公司金融服务
全球公司金融
公司融资服务
人民币结算服务
公司金融服务 | 个人金融服务 | 银行卡服务 | 电子银行服务
公司金融服务

钓鱼

- 每日新增拦截钓鱼网站数量突破6400个

- 与网购有关的钓鱼网站占比达到47%。而在虚假网购相关的钓鱼网站中，仅假彩票和假电商钓鱼网站就占了近90%。

钓鱼威胁

- 特点：
  - 骗术越来越高超，越来越曲折
  - 行骗过程步骤紧凑
  - 诱饵多元化

- 造成后果：
  - 对用户经济造成损失
  - 影响企业信用

法律风险

信用风险

资金托管风险

安全漏洞

钓鱼

作弊

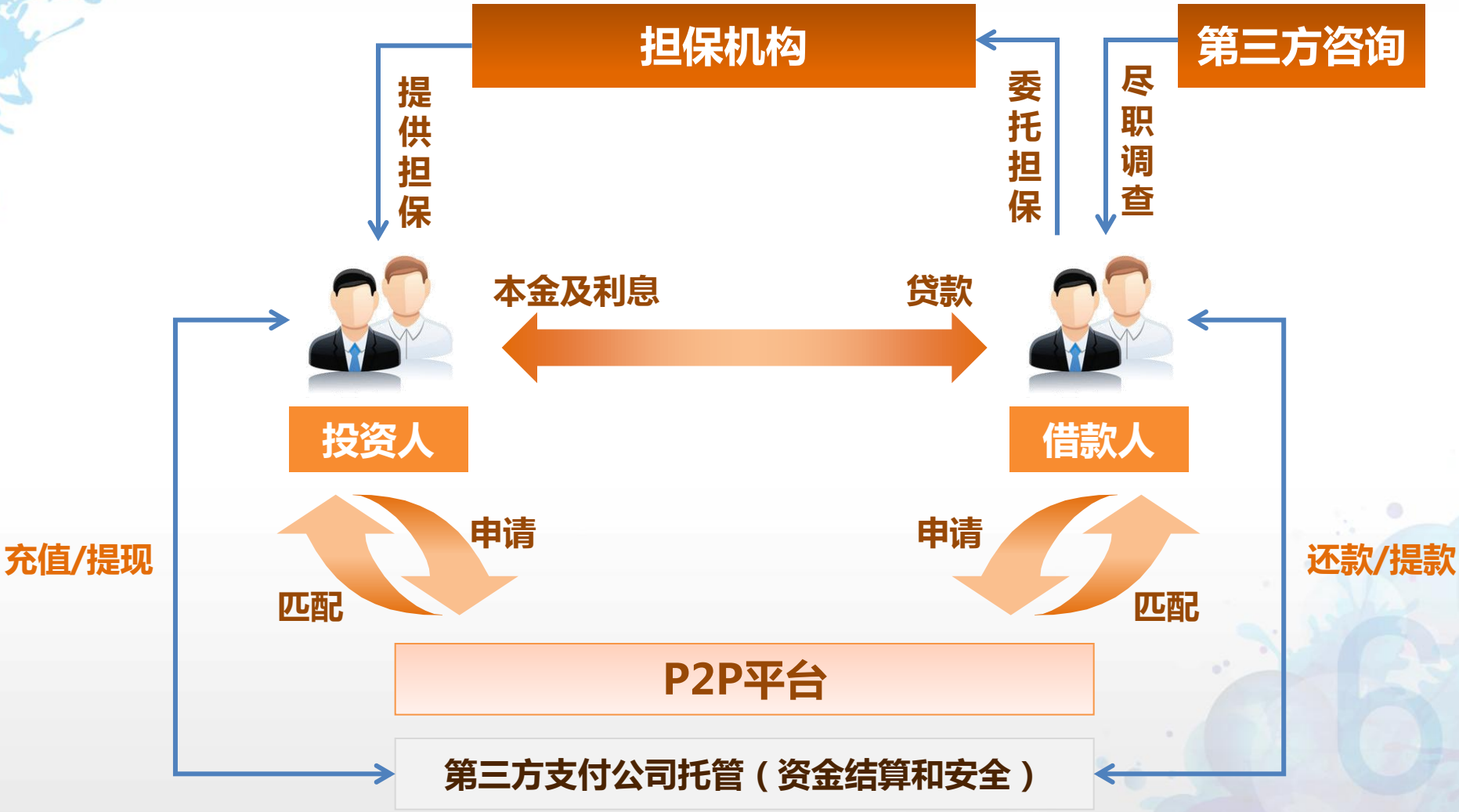
支付漏洞

……

如何预防？

业务风险预防

完善的网贷流程


担保机构
第三方咨询
提供担保
委托担保
尽职调查
本金及利息
贷款
投资人
借款人
申请
匹配
申请
匹配
充值/提现
还款/提款
P2P平台
第三方支付公司托管（资金结算和安全）

四重保障

借款人100%真实有效

借款人均经过严格筛选与专业审核，不同产品线采取不同的风控模式：与产业链核心企业合作，通过产业链大数据支持对产业链企业进行分析评判；与中国信贷旗下第一车贷合作，为优质二手车经销商提供融资，并以车辆作为反担保措施；与中国信贷旗下第一房贷合作，为在一二线城市拥有房产的经营业主提供融资，并以其名下房产作为反担保措施

第三方机构诚信承保

平台与国内知名担保公司合作，为投资人的本金与收益提供无限连带责任担保。一旦借款人发生违约，担保公司立刻启动代偿机制，优先保证投资人权益

无资金池模式规范运作

对借款人和投资人的资金进行匹配，确保借款人和投资人直接签订真实有效的借贷合同。平台只作为第三方中立机构，为借贷双方提供信息发布与资金匹配

第三方支付账号安全托管

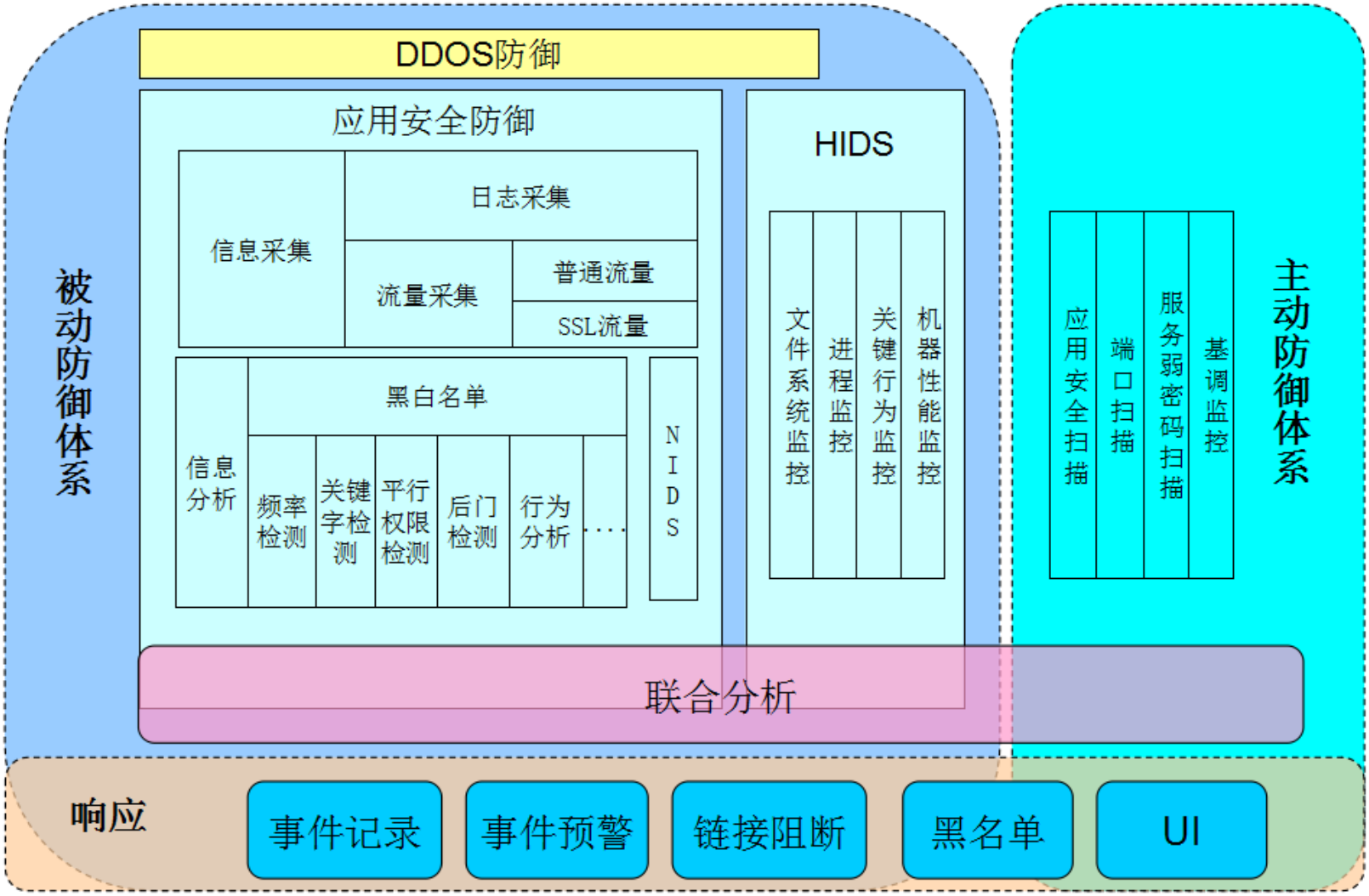
引入第三方支付机构对投资人资金进行监管，投资人的资金会自动划拨至第三方监管账户，而不会沉淀在第一P2P平台

产业链金融

- 与产业领域的核心龙头企业合作，结合核心企业提供的产业链大数据进行分析、评判，并针对不同行业、不同产业链量身定制打分卡模型，由专业的金融团队对借款项目进行严格筛选和风险把控。借款人均为核心企业产业链上下游的长期合作方，现金流稳定，经营状况良好。

技术风险预防

安全防御体系

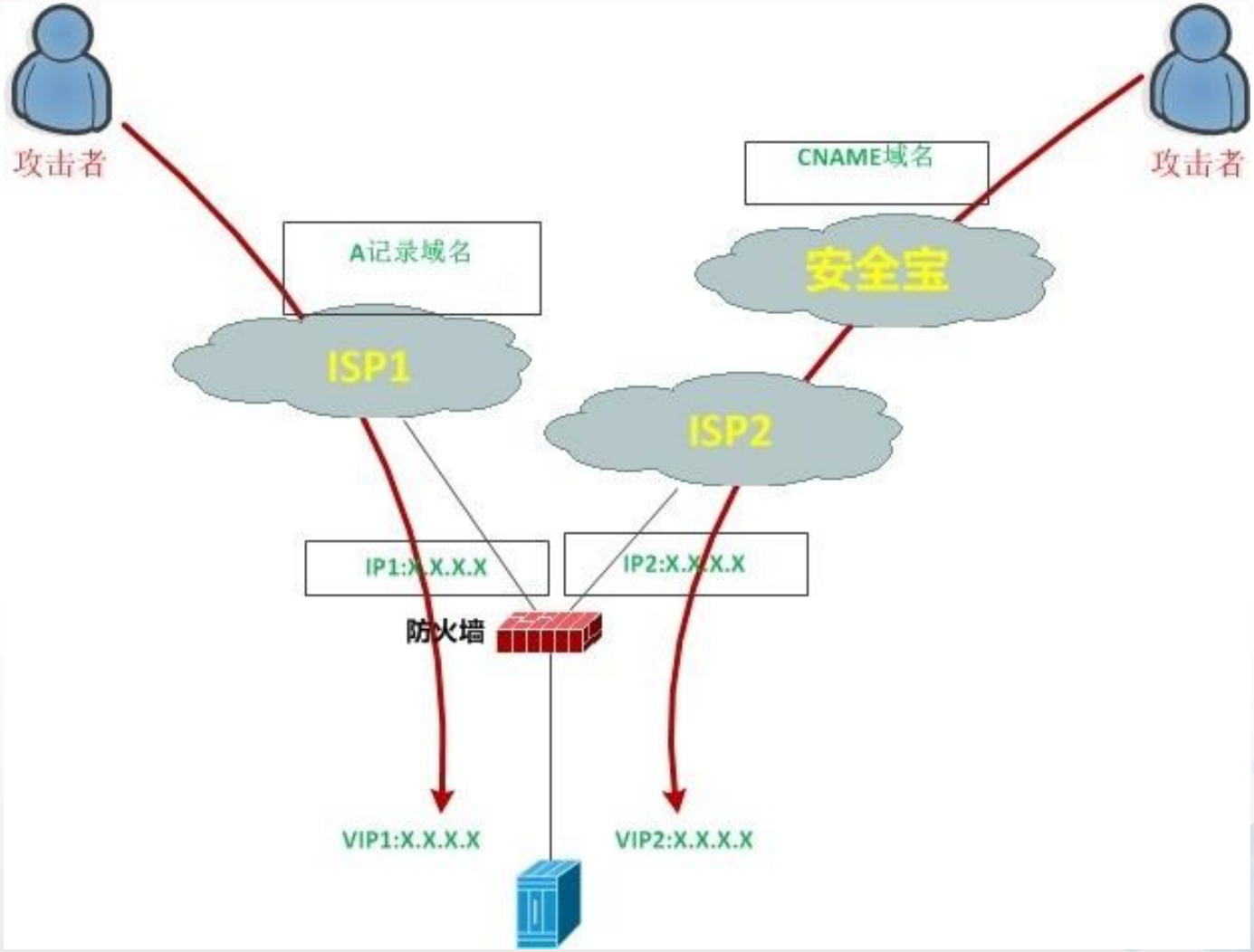

被动防御体系
DDOS防御
应用安全防御
信息采集
日志采集
流量采集
普通流量
SSL流量
信息分析
黑白名单
频率检测
关键字检测
平行权限检测
后门检测
行为分析
....
NIDS
HIDS
文件系统监控
进程监控
关键行为监控
机器性能监控
主动防御体系
应用安全扫描
端口扫描
服务弱密码扫描
基调监控
联合分析
响应
事件记录
事件预警
链接阻断
黑名单
UI

DDOS防御

DDOS防御方式

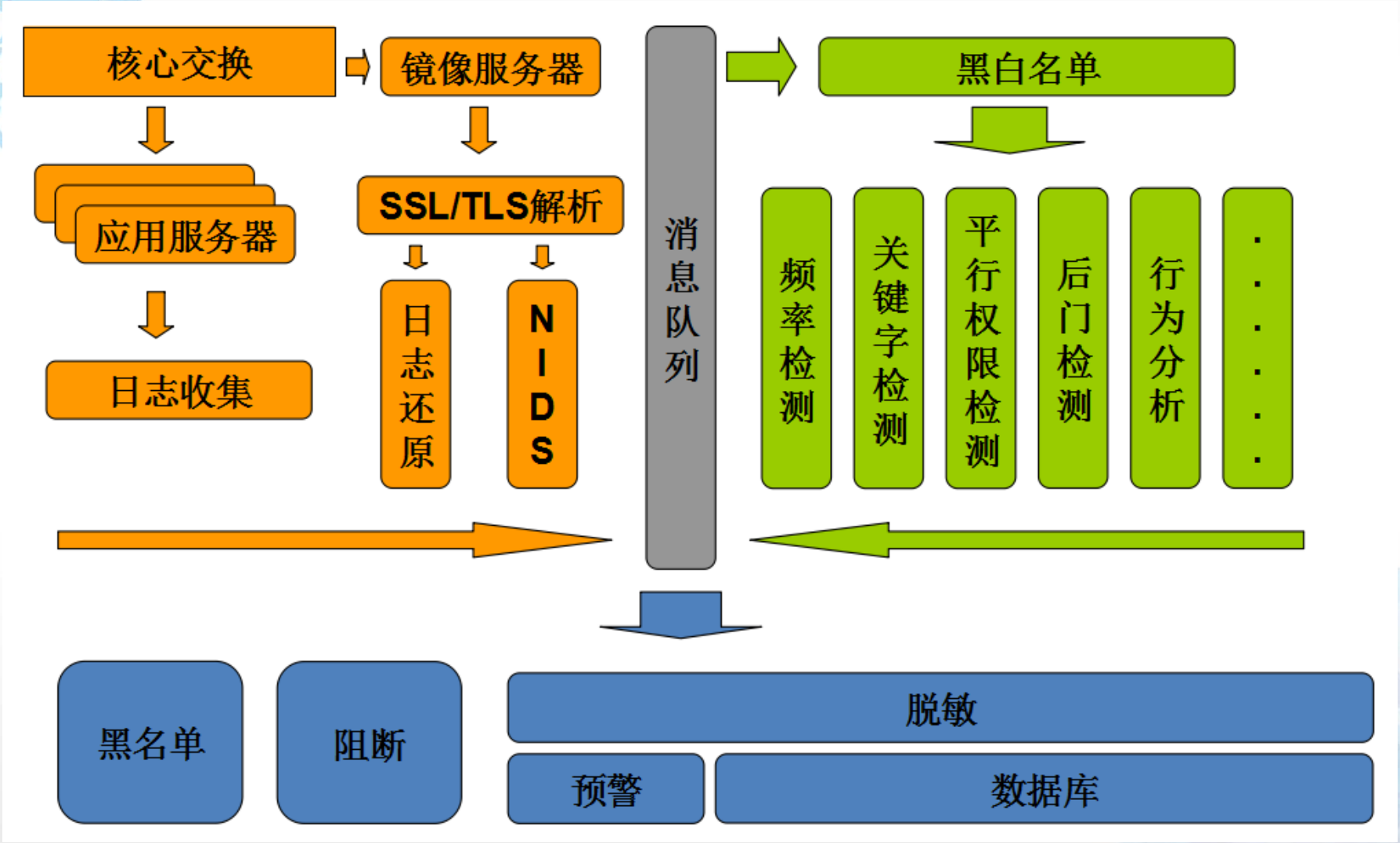
- 防CC攻击及服务攻击:
  - 防火墙
- 防流量攻击:
  - 阿里云/安全宝/加速乐/网站宝
  - 自建抗D中心
- 硬件和带宽成本的比拼

DDOS防御网络拓扑


攻击者
攻击者
CNAME域名
A记录域名
安全宝
ISP1
ISP2
IP1:X.X.X.X
IP2:X.X.X.X
防火墙
VIP1:X.X.X.X
VIP2:X.X.X.X

应用安全防御

应用安全防御体系


核心交换
镜像服务器
黑白名单
应用服务器
SSL/TLS解析
日志收集
日志还原
NIDS
消息队列
频率检测
关键字检测
平行权限检测
后门检测
行为分析
. . . . .
黑名单
阻断
脱敏
预警
数据库

日志采集

- 服务器日志收集
- 镜像流量重组

日志分析 -- 频率检测

检测内容：

- IP访问频率
- URL访问频率

```
src_ip_group_alert:
 common:
  win_time : 5
  min_request_count : 20
 response_status:
  below:
   #200 : 10%
  above:
   404 : 90%
 request_frequency:
  above: 3000
```

检测恶意行为：

- 扫描/爬虫
- 暴力登录
- 平行权限

日志分析 -- 关键字检测

检测内容：

- HTTP请求头中是否包含预定的关键字

检测恶意行为：

- 扫描
- 应用攻击

```
word_alert:
  word:
    all: [curl]
    url: [wp-login.php]
```

日志分析 -- 平行权限检测

如果一个提供用户资料的页面,未做资源授权限制:

www.xxx.com/user?id=1 或 www.xxx.com/user/info/1

则遍历ID即可便利此网站的用户

检测内容:

- 相同源IP的如下两种请求的频率:
  - 请求地址相同，关键参数不同
  - 请求地址相似，关键参数相同

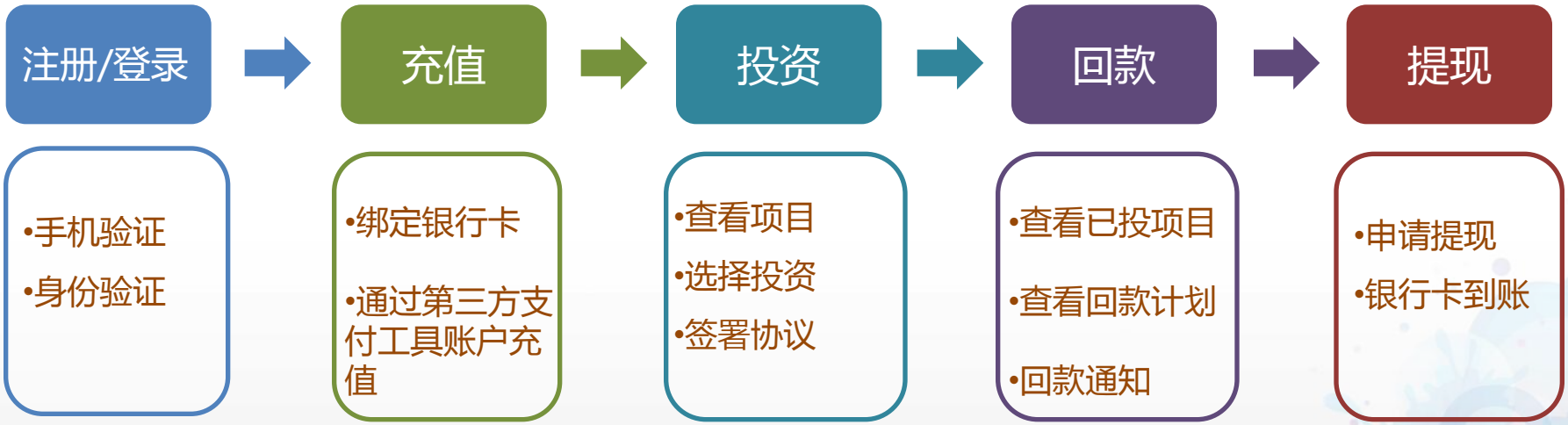
日志分析 -- 后门检测

- 长时间内，某URL仅被单一IP访问

```
request_url_group_alert:
  common:
    win_time : 480
    min_request_count : 1
  min_ip_count : 1
```

日志分析 -- 行为分析

- 正常的用户行为：



日志分析 -- 行为分析

- 异常的用户行为：

日志分析 -- 行为分析

- 检测内容：
  - 恶意攻击
  - 作弊
  - 钓鱼（IP异常，行为异常）
  - 业务逻辑漏洞

HIDS

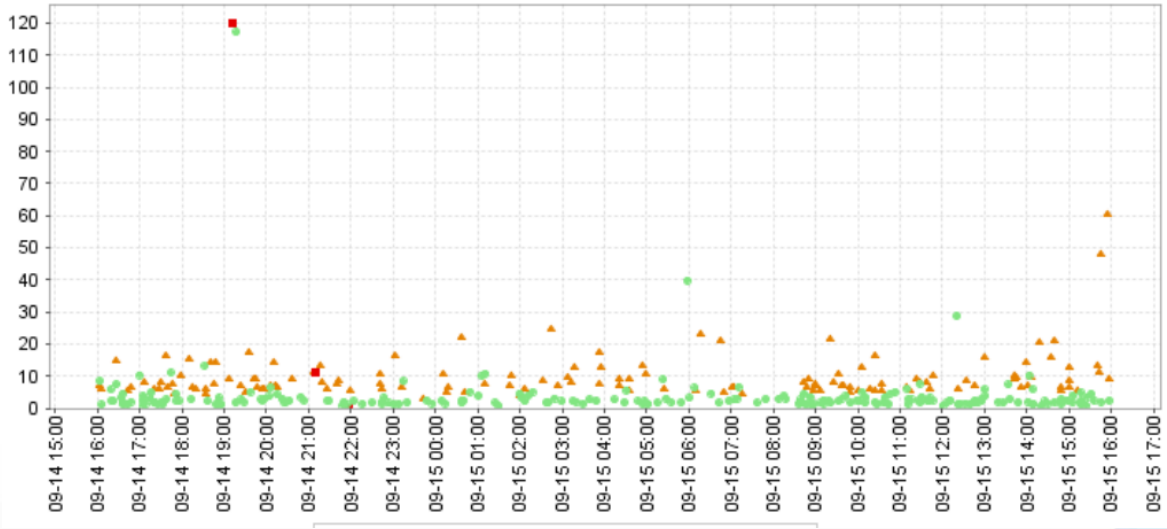
- 文件系统监控
  - inotify
- 进程监控
  - acct
- 关键行为监控
  - ssh等服务的登录/登出；mysql登录失败等等。
- 机器性能监控

主动防御体系

- 应用安全扫描
  - 用主流的WEB漏洞检测工具进行定时扫描
- 端口扫描
  - nmap/masscan
- 弱密码检测
  - hydra
- 基调

主动防御体系 -- 基调

- DNS劫持
- 代码注入
- IFRAME劫持
- 重定向劫持



响应

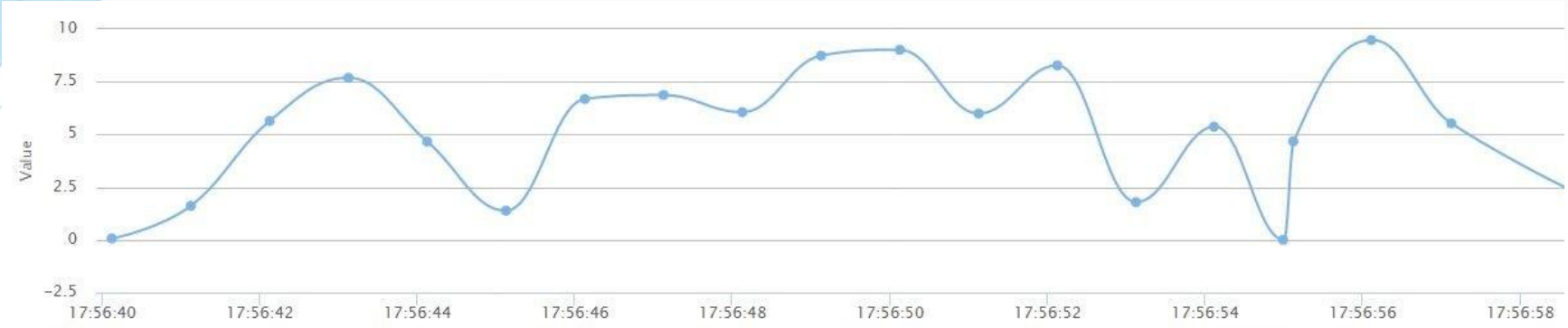
- 黑名单
  - 在公共cache中维护IP黑名单与用户黑名单
- 预警
  - 邮件预警
  - 短信预警
- 阻断
  - 旁路发送RST数据包
- 持久存储
  - 将日志与报警记录经过脱敏后持久存储到数据库中

响应 -- 邮件预警

jxq SQLMAP FOUND 1 分钟(2014-09-15 14:44:42---2014-09-15 14:45:42)攻击次数为 7

src	dst	total	src_count
106.186.122.44[日本]	[redacted][局域网对方和您在同一内部网]	7	0

实时日志分析预警



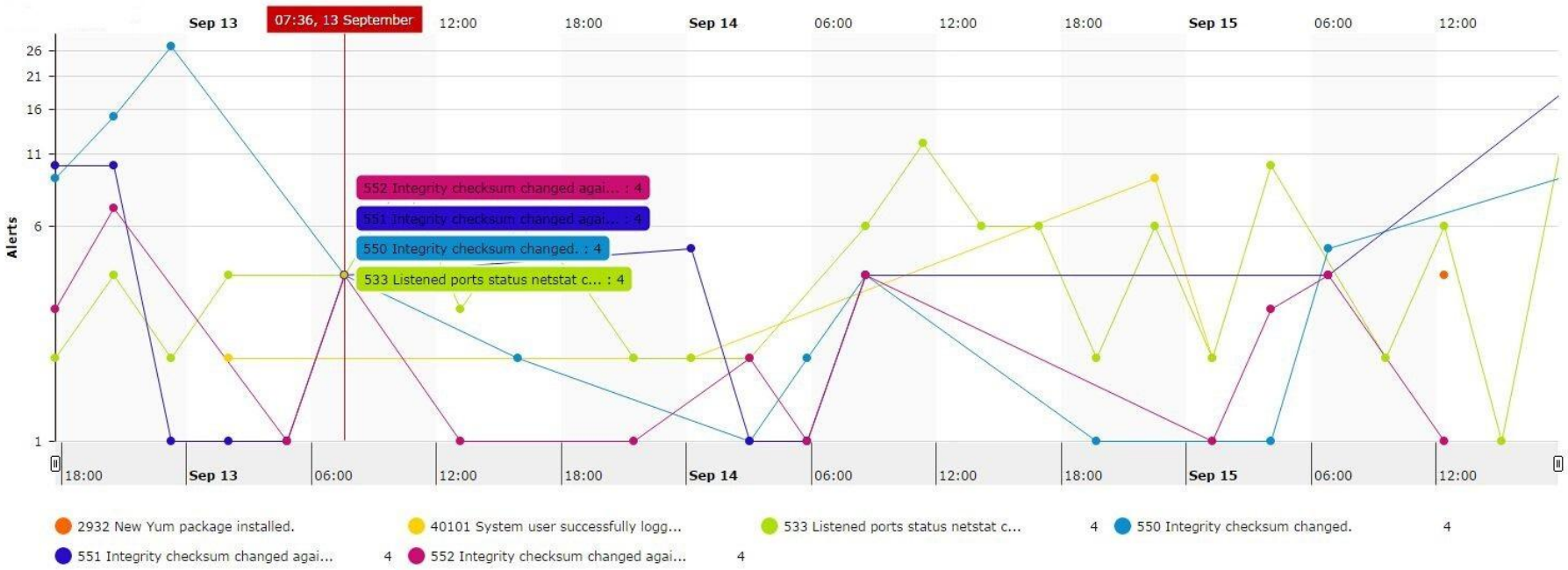
Hover rows

IP	Time	报警种类	报警说明	冗余报警说明
175.6.8.83	2014-09-15 17:55:29	request_frequency_alert		
175.6.8.83	2014-09-15 17:53:11	request_frequency_alert		
211.90.30.161	2014-09-15 17:49:20	request_frequency_alert		
211.90.30.161	2014-09-15 17:49:19	request_frequency_alert		
175.6.8.83	2014-09-15 17:49:20	request_frequency_alert		
175.6.8.83	2014-09-15 17:49:18	request_frequency_alert		
211.90.30.161	2014-09-15 17:49:16	request_frequency_alert		
175.6.8.83	2014-09-15 17:49:17	request_frequency_alert		

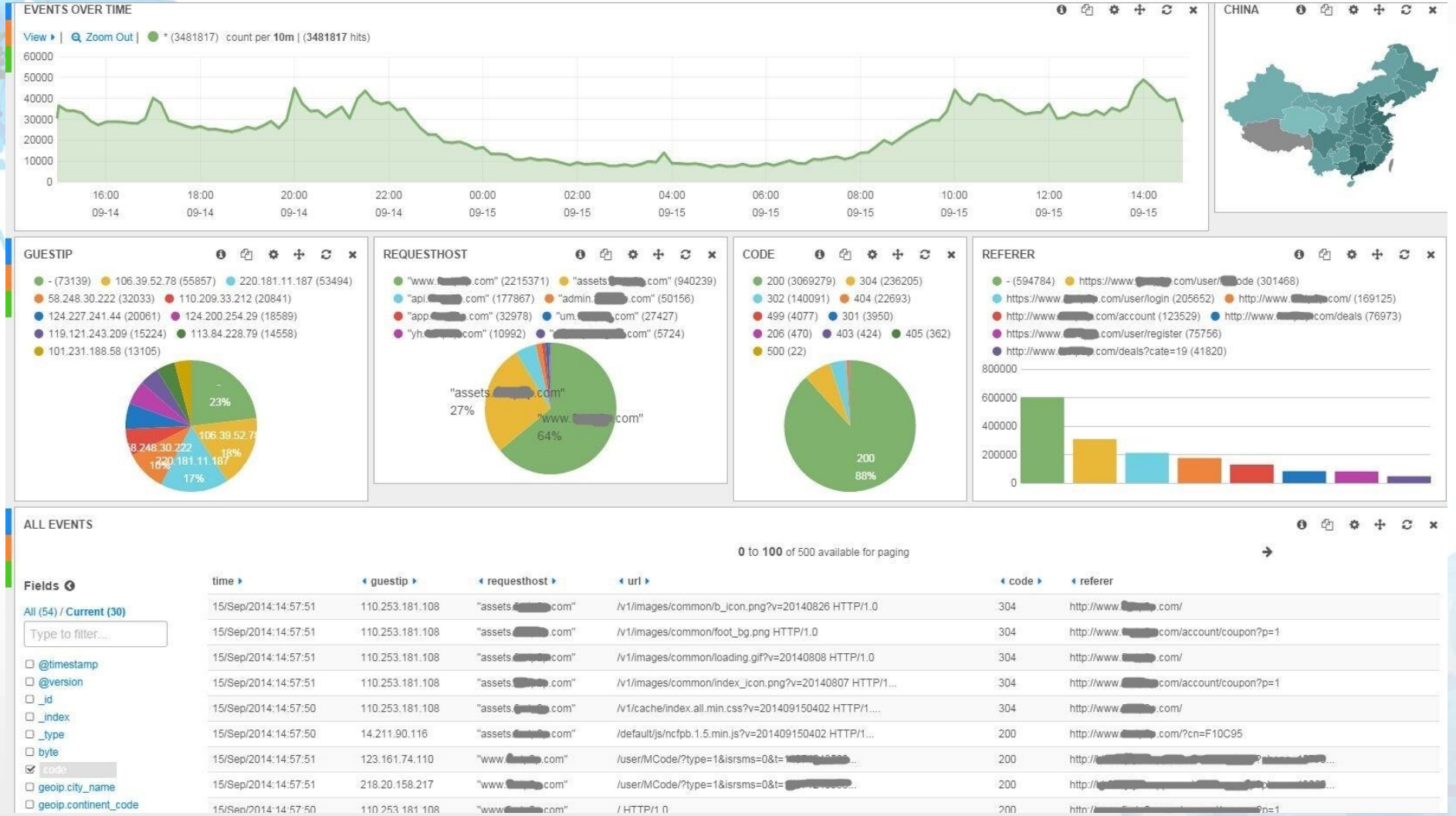
NIDS预警


Dashboard
More Options
LAST 24 TODAY YESTERDAY LAST WEEK THIS MONTH THIS QUARTER THIS YEAR
Updated: 09/15/14 05:47 PM CST
55094
HIGH SEVERITY
55,094 / 59,820
4469
MEDIUM SEVERITY
4,469 / 59,820
257
LOW SEVERITY
257 / 59,820
Sensors
Severities
Protocols
Signatures
Sources
Destinations
Event Count vs Time By Sensor
BEIJING
12,500
10,000
7,500
5,000
2,500
0
-2500
Event Count
BEIJING
957 Events
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Hour of Day
TOP 5 SENSOR
BEIJING 2,641,490
TOP 5 ACTIVE USERS
Administrator 0
LAST 5 UNIQUE EVENTS
ET POLICY Http Client Bod... 440,702
ET WEB_SERVER Outbound PH. 669,396
ET POLICY Java Url Lib Us... 16,449
SURICATA STREAM TIMEWAIT ... 3,688
ET MALWARE Suspicious Use... 37,072
ANALYST CLASSIFIED EVENTS
Unauthorized Root Access 0
Unauthorized User Access 0
Attempted Unauthorized... 0
Denial of Service Attack 0
Policy Violation 0
Reconnaissance 0
Virus Infection 0
False Positive 0

HIDS预警


Sep 13
07:36, 13 September
12:00
18:00
Sep 14
06:00
12:00
18:00
Sep 15
06:00
12:00
Alerts
26
21
16
11
6
1
552 Integrity checksum changed agai... : 4
551 Integrity checksum changed agai... : 4
550 Integrity checksum changed. : 4
533 Listened ports status netstat c... : 4
18:00
Sep 13
06:00
12:00
18:00
Sep 14
06:00
12:00
18:00
Sep 15
06:00
12:00
2932 New Yum package installed.
40101 System user successfully logg...
533 Listened ports status netstat c... 4
550 Integrity checksum changed. 4
551 Integrity checksum changed agai... 4
552 Integrity checksum changed agai... 4

持久化存储


EVENTS OVER TIME
View | Zoom Out | * (3481817) count per 10m | (3481817 hits)
60000
50000
40000
30000
20000
10000
0
16:00 09-14
18:00 09-14
20:00 09-14
22:00 09-14
00:00 09-15
02:00 09-15
04:00 09-15
06:00 09-15
08:00 09-15
10:00 09-15
12:00 09-15
14:00 09-15
CHINA
GUESTIP
- (73139) 106.39.52.78 (55857) 220.181.11.187 (53494)
58.248.30.222 (32033) 110.209.33.212 (20841)
124.227.241.44 (20061) 124.200.254.29 (18589)
119.121.243.209 (15224) 113.84.228.79 (14558)
101.231.188.58 (13105)
23%
18%
17%
REQUESTHOST
"www.[redacted].com" (2215371) "assets[redacted].com" (940239)
"api.[redacted].com" (177867) "admin.[redacted].com" (50156)
"app[redacted].com" (32978) "um.[redacted].com" (27427)
"yh.[redacted].com" (10992) "[redacted].com" (5724)
"assets[redacted].com"
27%
"www.[redacted].com"
64%
CODE
200 (3069279) 304 (236205)
302 (140091) 404 (22693)
499 (4077) 301 (3950)
206 (470) 403 (424) 405 (362)
500 (22)
200
88%
REFERER
- (594784) https://www.[redacted].com/user/[redacted]ode (301468)
https://www.[redacted].com/user/login (205652) http://www.[redacted].com/ (169125)
http://www.[redacted].com/account (123529) http://www.[redacted].com/deals (76973)
https://www.[redacted].com/user/register (75756)
http://www.[redacted].com/deals?cate=19 (41820)
800000
600000
400000
200000
0
ALL EVENTS
0 to 100 of 500 available for paging
Fields
All (54) / Current (30)
Type to filter...
@timestamp
@version
_id
_index
_type
byte
code
geoip.city_name
geoip.continent_code
time | guestip | requesthost | url | code | referer
15/Sep/2014:14:57:51 110.253.181.108 "assets[redacted].com" /v1/images/common/b_icon.png?v=20140826 HTTP/1.0 304 http://www.[redacted].com/
15/Sep/2014:14:57:51 110.253.181.108 "assets[redacted].com" /v1/images/common/foot_bg.png HTTP/1.0 304 http://www.[redacted].com/account/coupon?p=1
15/Sep/2014:14:57:51 110.253.181.108 "assets[redacted].com" /v1/images/common/loading.gif?v=20140808 HTTP/1.0 304 http://www.[redacted].com/
15/Sep/2014:14:57:51 110.253.181.108 "assets[redacted].com" /v1/images/common/index_icon.png?v=20140807 HTTP/1... 304 http://www.[redacted].com/account/coupon?p=1
15/Sep/2014:14:57:50 110.253.181.108 "assets[redacted].com" /v1/cache/index.all.min.css?v=201409150402 HTTP/1.... 304 http://www.[redacted].com/
15/Sep/2014:14:57:50 14.211.90.116 "assets[redacted].com" /default/js/ncfpb.1.5.min.js?v=201409150402 HTTP/1... 200 http://www.[redacted].com/?cn=F10C95
15/Sep/2014:14:57:51 123.161.74.110 "www.[redacted].com" /user/MCode/?type=1&isrsms=0&t=[redacted] 200 http://[redacted]
15/Sep/2014:14:57:51 218.20.158.217 "www.[redacted].com" /user/MCode/?type=1&isrsms=0&t=[redacted] 200 http://[redacted]
15/Sep/2014:14:57:50 110.253.181.108 "www.[redacted].com" / HTTP/1.0 200 http://[redacted]

本人邮箱： liufr.vle@gmail.com

特别致谢：
LION_00

Q&A

THANKS

SequeMedia 盛拓传媒 | IT168 www.it168.com | ChinaUnix | ITPUB