Docker 的日志收集

刘卓 HanSight瀚思

2016 年 3月23

HanSight 瀚思

企业背景

HanSight 瀚思

- 成立于 2014 年的创业公司
- **数据驱动安全** – 以大数据分析的方式解决安全问题
- 创始人来自趋势科技、天云、微软、 Oracle

- 两大类产品线：**企业版**和 **SaaS** 版
- 企业版销售对象是各种大型企业总部、事业单位等
- 基于 Elasticsearch 1.5
- 重点在性能、安全、算法

- SaaS 版 – **安全易** – 面向中小企业
- 云端的多租户 SIEM
- 基于 Elasticsearch 1.7 + Kibana 4.1 改编
- 重点在可视化

瀚思专注于大数据安全分析

- 已拥有招商银行、公安部、天津公安、北京联通、河北金融学院、北京燃气集团等十余家客户，涵盖公安、金融、电信、制造、政府等领域。

- 积极拓展大数据安全行业与标准联盟，包括加入《CNCert中国互联网网络安全威胁治理联盟》，与公安部三所共同制定大数据安全体系标准，参与制定数据治理国家标准，与华为达成大数据生态战略合作等。

- 瀚思于2015年获得美国硅谷Red Herring全球创新公司百强、亚洲创新公司百强，为上榜唯一中国安全企业。2015中国信息产业年度人物获得者。

RED HERRING GLOBAL WINNER 100

CNCERT/CC 国家互联网应急中心

中华人民共和国公安部 The Ministry of Public Security of the People's Republic of China

HanSight 瀚思

Docker 的日志处理

1. 为什么要采集日志
   - 概述日志收集的目的
2. 传统linux日志收集、处理
   - 收集方式
   - 处理方式
3. docker日志采集方法的演变
   - docker v1.6之前
   - docker v1.6之后
   - 演示
4. 日志简单分析
   - RPCA算法

Q&A

Log, Why?

- 为了跟踪、定位、排除故障，需要了解服务程序故障位置的上下文
- 监控服务，定时更新服务状态，实现运维预警
- 性能优化依据，实时获取机器环境，如CPU使用率，内存消耗量和网络性能
- 利用机器学习与预测，辅助业务决策

传统linux采集、处理日志的方式

- 采集：

  * 建立一个中央日志服务器，修改客户端日志配置文件，将日志备份到服务器上。（使用syslog 或者rsyslog ）

    [root@wwwserver /]# vi /etc/syslog.conf

    添加下面的代码到syslog.conf中:*.* @logserver

  * 或者安装数据库，进行日志数据库管理。

- 处理：

  * 以手动方式搜索日志文件，find、grep、awk、sed、tail、cut

  * logsurfer、swatch

Docker 怎样?

docker日志采集方法的演变

Docker v1.6之前:

- 存储方式：
  1. Docker仅仅是从容器中采集stdout和sterr
  2. 用JSON进行简单的封装并存储到磁盘

- 日志采集的演进：
  1. Docekr的早期使用者会采集 /var/lib/docker/containers/**

     缺点：必须用root用户才能得到
  2. 之后较好的用户体验方式：docker logs， 直接使用获取日志的 daemon API
  3. logspout开源项目的出现， 对接API，转发syslog

Docker日志采集的开源项目和服务

Logspout

cAdvisor

Datadog

Diamond(Cgroup)

Graphite / Grafana

Example：

转发所有docker容器的日志到远程的syslog：

```
docker run --name="logspout" \
        --volume=/var/run/docker.sock:/var/run/docker.sock \
        gliderlabs/logspout \
        syslog://logs.papertrailapp.com:55555
```

方式总结：

- 应用程序直接将log上传入日志服务器

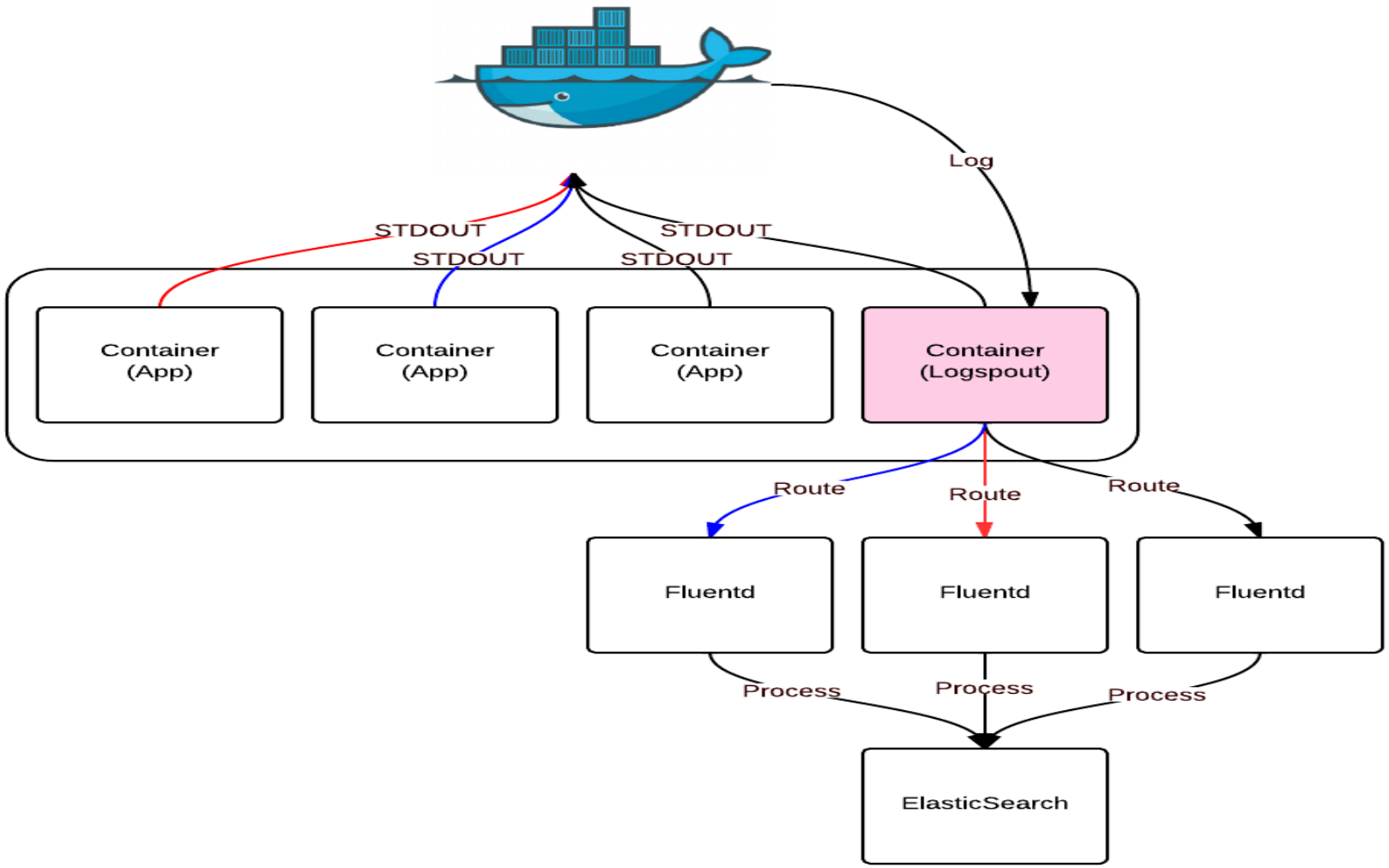
  es 插件　'com.internetitem:logback-elasticsearch-appender:1.2’

- Log写入一个挂载在docker上的文件
- 安装系统日志采集器
  - docker exec 注入采集器
  - Curl -XGET /containers/(id)/logs
- 直接写入在 /var/lib/docker/containers/**

缺点：

- 所有日志都在 json-file 中
- 文件大小持续增长，缺省不能拆分
- 多个容器一起收集时，无法自然区分

Docker 日志采集架构



Docker v1.6之后

引入日志驱动器(Log Drivers)，除了默认json-file外，还支持： 将日志写入syslog、 journald、gelf、 fluentd、 awslogs、 splunk、 null，以及其他指定方式（如Hansight）

docker daemon --log-driver=journald

docker run --log-driver=journald ...

docker run –logs-driver null 就是屏蔽掉日志,不进行输出

使用 Log Driver

- Json-file :

  --log-opt max-size=[0-9+][k|m|g]　设置文件大小

  --log-opt max-file=[0-9+]　　文件日志保留数量

- Syslog：

--log-opt syslog-address=[tcp|udp|tcp+tls]://host:port

  --log-opt syslog-address=unix://path

  --log-opt syslog-tls-ca-cert=/etc/ca-certificates/custom/ca.pem

  --log-opt syslog-tls-cert=/etc/ca-certificates/custom/cert.pem

  --log-opt syslog-tls-key=/etc/ca-certificates/custom/key.pem

  --log-opt syslog-tls-skip-verify=true

- gelf:

  --log-opt gelf-address=udp://host:port

  --log-opt tag=“database”

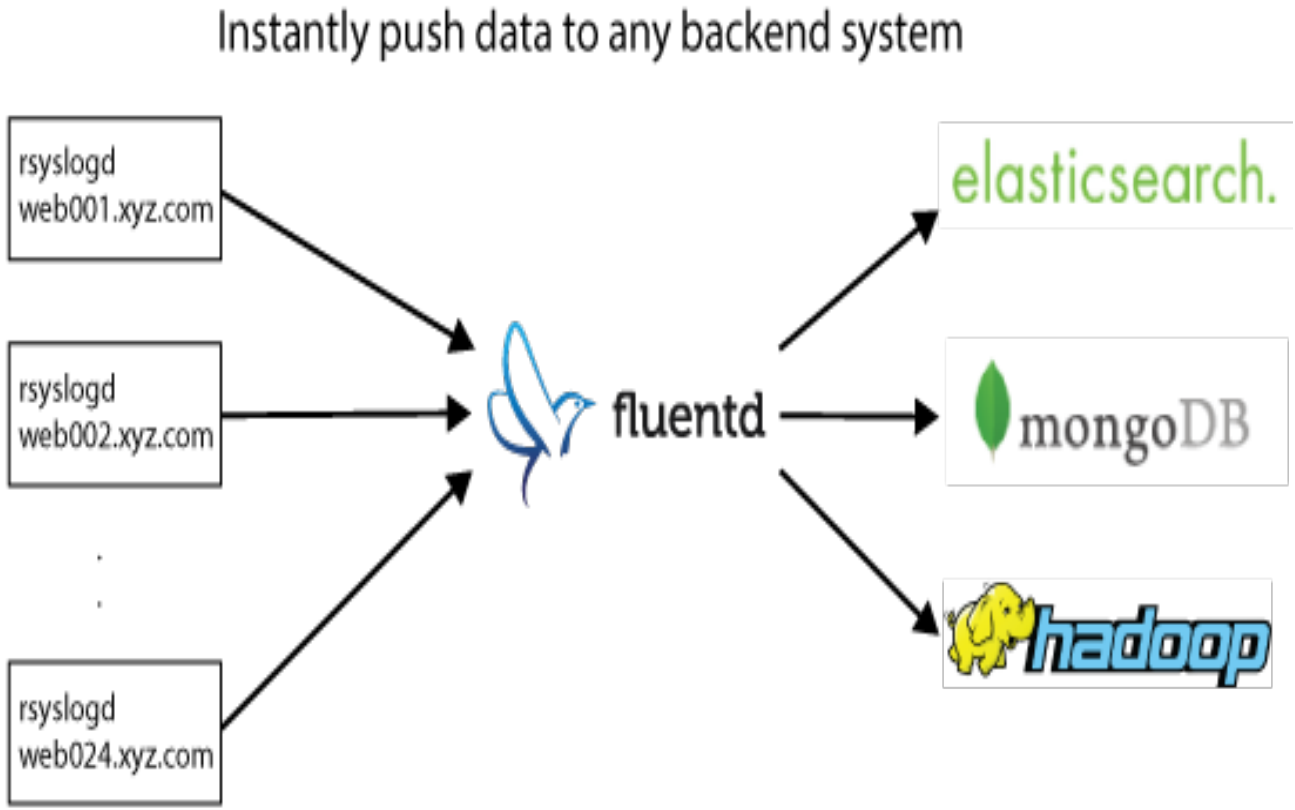
多个容器之间共享syslog进程，传送到 log driver

标记	描述
{{.ID}}	容器Id的前12个字符
{{.FullID}}	容器Id
{{.Name}}	容器名字
{{.ImageID}}	容器的image Id的前12个字符
{{.ImageFullID}}	容器的image ID
{{.ImageName}}	容器的image所使用的名字

--log-opt tag="{{.ImageName}}/{{.Name}}/{{.ID}}"

Aug 7 18:33:19 HOSTNAME docker/hello-world/foobar/5790672ab6a0[9103]: Hello from Docker.

架构和集群演示



日志的处理： 用户行为异常检测

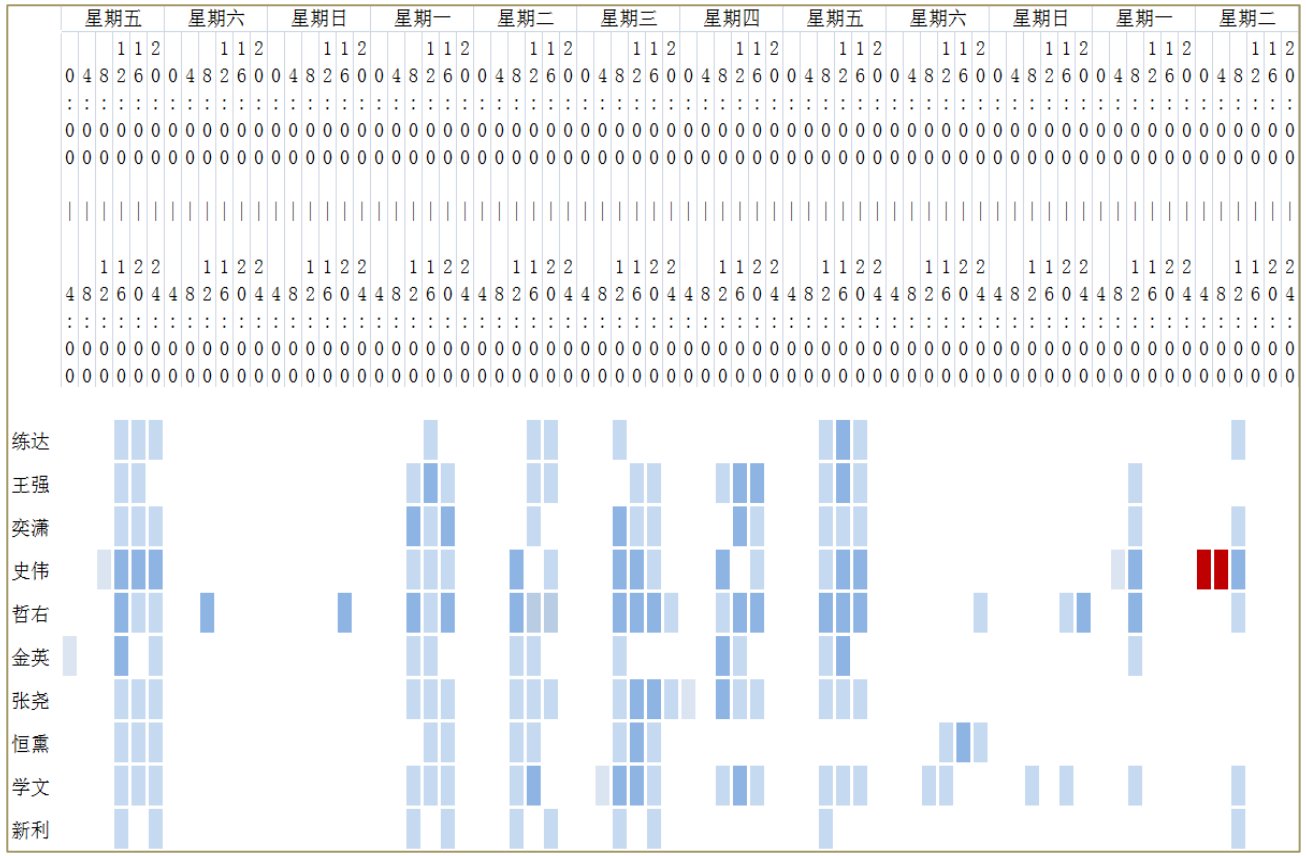
挑战：

随着移动办公和BYOD的普及，企业越来越难从正常的行为找出被盗用的账号行为。

解决方法

自动建立特定用户的画像，包括他的合法行为白名单和行为基线

用户行为分析引擎侦测用户的异常行为，例如从可疑位置登录，或是访问和平时完全不同的数据或数据量，或是把数据上传至公司外部的可疑地址，系统可以提供该用户最近的所有行为给安全管理员进行进一步的详细调查

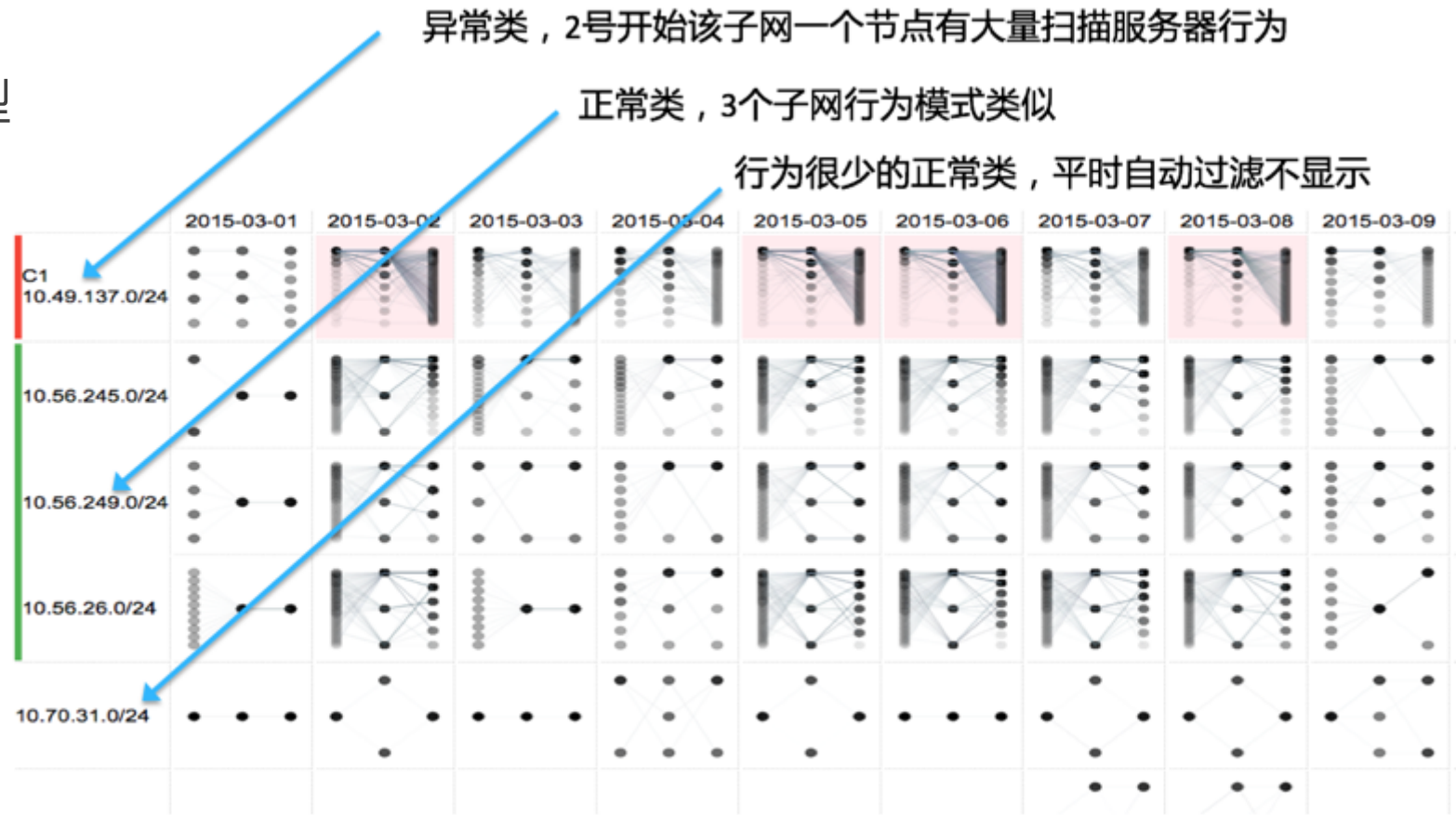


日志的处理：低速扫描

威胁名称：低速扫描
数据输入：防火墙日志
检测对象：重要服务器长周期通信模型

分析过程：

- 用户自定义需要分析的服务器和周期；
- 利用多变量时间序列聚类算法，把源IP按目的端口和目的IP的通讯行为聚合成多类，过滤无异常的类；
- 一张图上可视化每类的每天变化情况，用户可精确定位到具体IP、目的端口、时间；



算法处理后的海量IP的长周期通讯模式图

日志的处理：交易异常

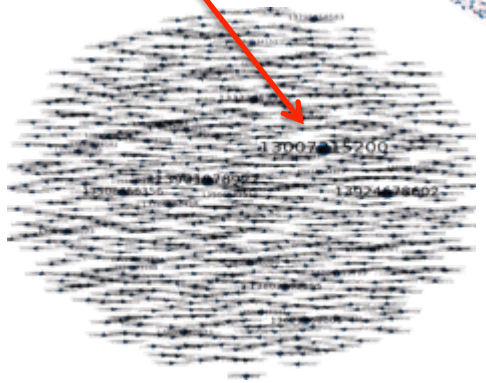
威胁名称：资金转入转出异常

分析过程：

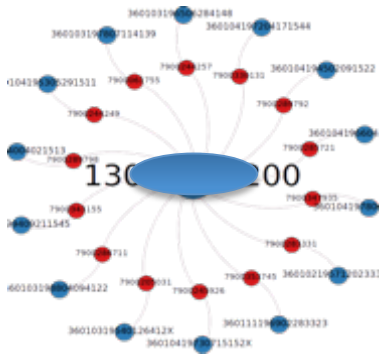
- 自定义分析的网银交易日志周期；
- 将海量用户手机号、账户号和身份证号码进行关联并可视化展示；
- 发现盗用大量身份证频繁开户的用户；进一步钻取分析，查看到可疑的用户手机号及所有相关的账户和身份证号；
- 同时发现相关账户有金融业务风险中的“火山”和“黑洞”情况出现；

第一步：建立数据模型

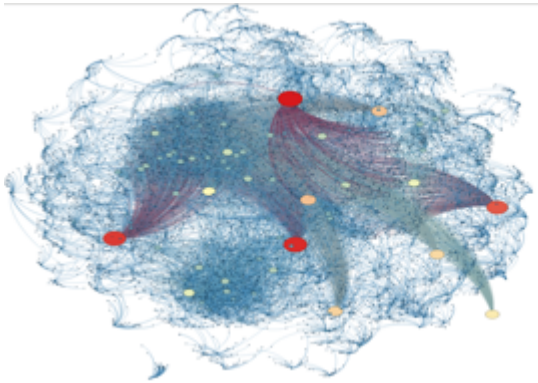
第二步：发现可疑号码



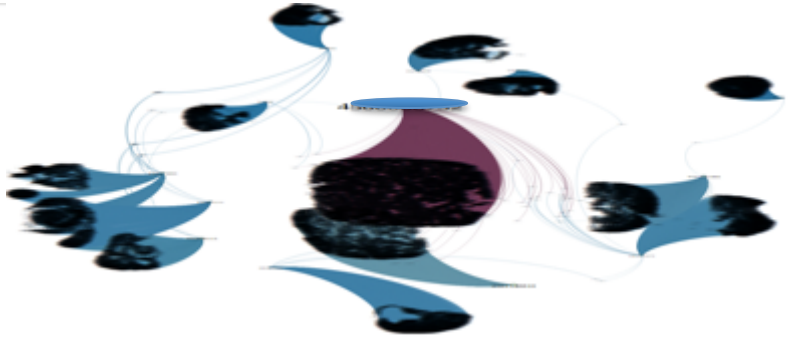
第三步：钻取关联分析



黑洞模型：账户大量转入交易



火山模型：账户大量转出交易



谢谢 | HanSight 瀚思

www.HanSight.com

微信公众号：瀚思安信

北京市海淀区中关村软件园9号楼2区306A

日志的处理 RPCA算法