女性移动App安全攻防战

黄益聪
美柚技术总监

主办单位：杭州 Alibaba Group 阿里巴巴集团 战略合作伙伴：intel

- 2015-今 **美柚技术总监**
- 2013 - 2015 **阿里巴巴(中国)软件有限公司 高级技术专家** 负责阿里云大数据基础服务核心开发 **阿里罗汉堂 讲师**，拥有6项技术发明专利
- 2005 - 2013 **英特尔公司 高级软件工程师** 负责高并发、海量数据、高性能场景的性能分析和优化，拥有一项美国专利，获得2011年英特尔中国EOY Award（英特尔中国个人最高奖项），在IEEE和多个国际技术会议发表论文和演讲

Meet you 美柚　Alibaba Group 阿里巴巴集团　intel

目 录
content

扫码观看大会视频

美柚

让女人更美更健康

厦门 * 杭州 * 上海

A

以**美柚(经期管理)**切入女性市场，又陆续推出了**柚宝宝孕育、柚宝宝时光、柚子街**等一系列软件，形成**工具＋社区＋电商**的闭合商业模式。

B

产品用户**超过1亿**，DAU超过**700万**，是国内最大的女性经期管理工具，也是第一大女性社区；是唯一一家覆盖从经期到孕期育儿等**女性完整生命周期的互联网公司。**

扫码观看大会视频

美柚家族App

美柚

柚子街

柚宝宝孕育

柚宝宝时光

扫码观看大会视频

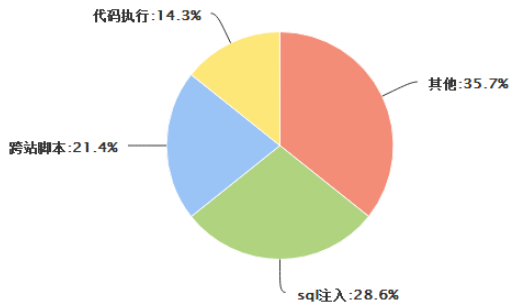
攻击概况

- 流量攻击
- 恶意CC攻击
- 撞库注册用户
- 刷短信
- 爬虫抓取
- 域名劫持、页面篡改

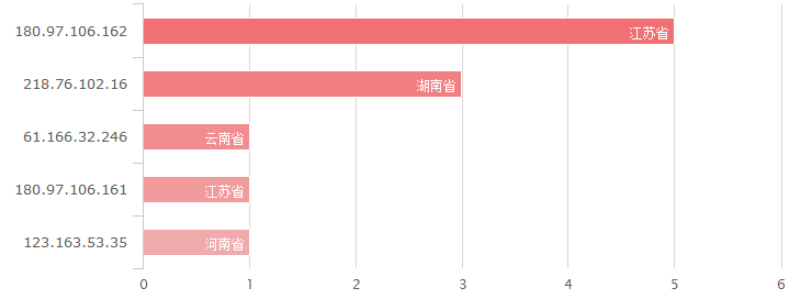
部分攻击统计

峰值流量	DDoS攻击防护次数	CC攻击防护次数	WEB攻击防护次数
< 1 Gb	92 次	12618 次	32272 次

攻击分类



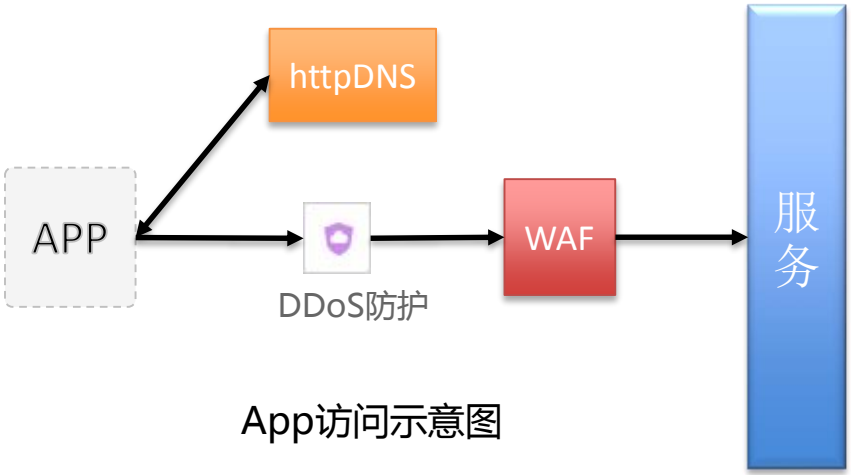
攻击源统计



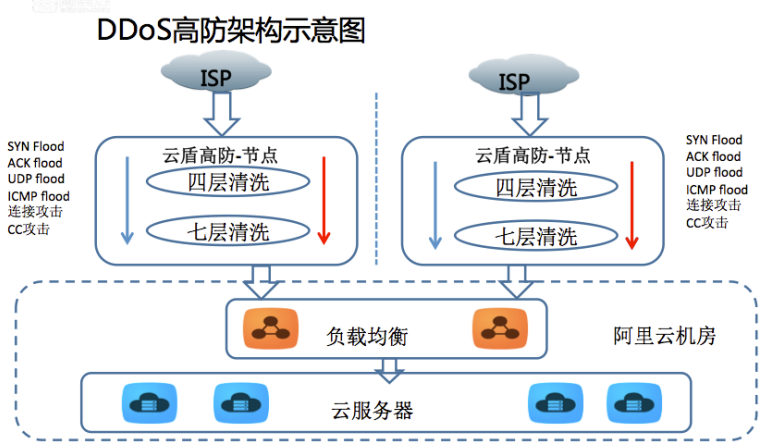
扫码观看大会视频

二、安全防御体系

DDoS防护



App访问示意图



- 阿里云DDoS防护：防护SYN Flood、UDP Flood、ACK Flood、ICMP Flood、DNS Query Flood、NTP reply Flood、CC攻击、WEB应用攻击等3到7层攻击

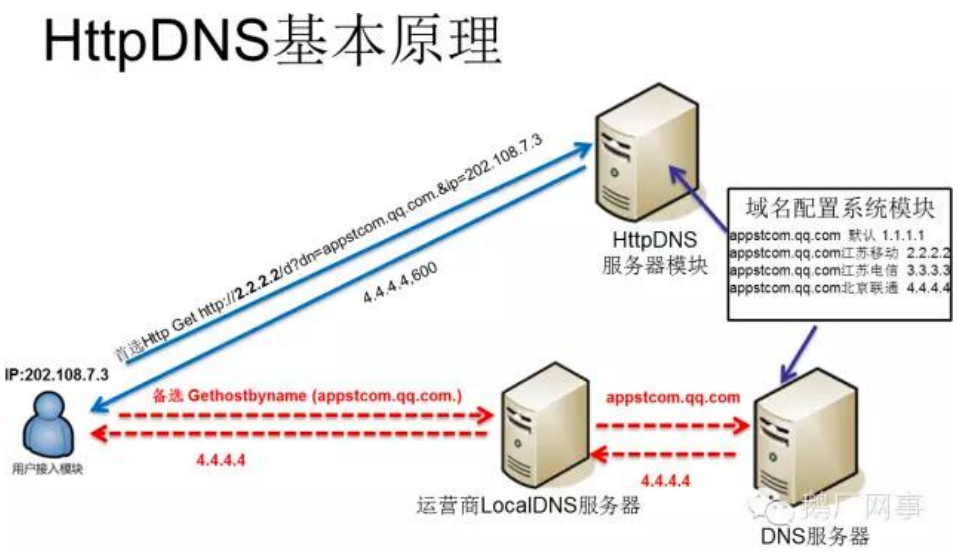
扫码观看大会视频

App安全

- 代码混淆
- 安全加固（阿里聚安全）
- 防重打包
- 模拟器识别：加入多维特征识别

自建HTTPDNS服务 + HTTP 2.0

- 防劫持
- 精准调度
- 0 ms解析延迟
- 快速生效
- 降低解析失败率
- 使用Post zip
- Keep Alive
- 更安全的SSL，防页面篡改



国内互联网根域出现重大故障 大量网站无法打开

2014年01月21日 16:12

来源：凤凰科技

13028人参与 1636评论

凤凰科技讯 1月21日消息，今日下午15:10左右，有网友称国内众多网站出现无法访问的现象。据部分网站管理员称，此次断网是因国内域名解析的根服务器出现问题，导致大量网站域名解析不正常。

故障具体表现在域名访问请求被跳转到几个没有响应的美国IP上，不同省份的用户均出现不同程度的网络故障。据悉，原因可能在于目前国际节点出现故障，国内三分之二DNS处于瘫痪状态。

弱网更流畅的用户体验

未优化-2G

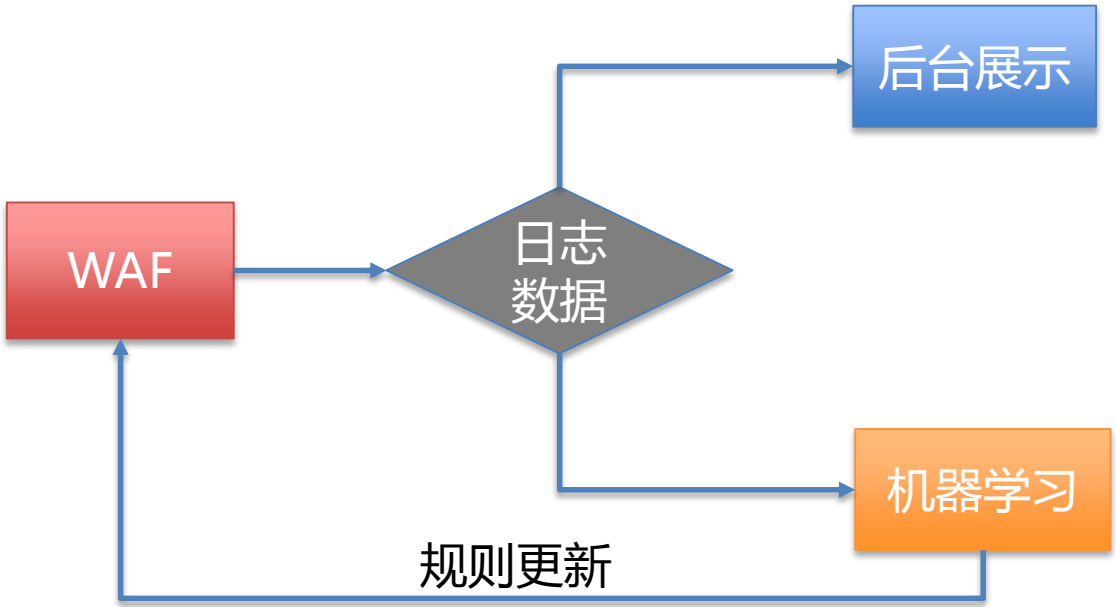
深度优化-2G

扫码观看大会视频

自研WAF（web application firewall）

- 基于openresty构建
- 高性能：得益于nginx的高性能，可横向扩展
- 灵活配置：使用lua开发，得益于脚本的灵活性，同时使用了lua jit兼顾了高性能
- 实时上线：可视化规则编辑，变更实时同步至所有worker，使用redis的subscribe/publish实现对worker广播，瞬间部署，无需重启
- 定制化防御功能：缓解CC攻击、精准访问控制、过滤非法请求，实时解决垃圾注册、刷库撞库、活动作弊、论坛灌水等严重业务风险

WAF演进



- 后台实时汇总展示
- 机器学习动态更新规则

扫码观看大会视频

三、社区反垃圾

社区风险

- 全国最大的女性社区—她她圈
- 日均浏览量过亿
- 广告贴、色情图、刷回复
- 盗号、卖号猖獗

扫码观看大会视频

反垃圾防控系统

业务

她她圈 | 蜜友圈 | 资讯 | IM | 个人资料 | 其他UGC

规则引擎

规则中心

- 文本规则：has | 相似文本 | 分类词库 | 机器学习
- 图片规则：相似算法 | OCR | 黄图算法 | 广告算法
- 用户规则：黑名单 | 白名单 | 用户评分 | 设备库
- 行为规则：高频 | 访问路径 | 浏览比 | 人机识别

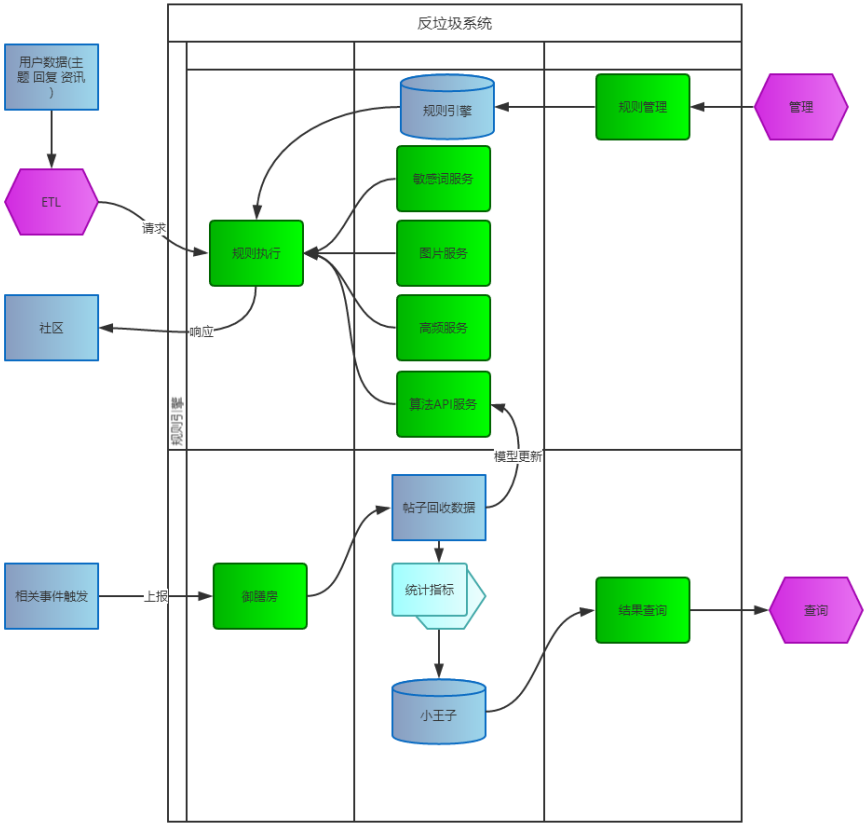
词库 | 图库 | 文本库 | 名单库 | 地址库

运营

规则配置 | 议程管理 | 执行引擎 | 规则监控 | 分析评测

反垃圾系统架构

- 图片服务：相似图片算法 + 阿里绿网
- 算法API服务：离线训练 + 在线模型更新
- 高频规则：Simhash
- 垃圾词挖掘



2016 The Computing Conference

THANKS