

移动开发构架漫谈 - - 反劫持实战篇

汽车之家 移动团队 莫松 2015年5月30日

汽车之家 移动团队 莫松

邮箱 : mosong@autohome.com.cn

微信 : 39151738

- 1.大家的app产品中多少使用http通信协议的？
- 2.app产品用户是否遭遇到网络劫持的情况？

目录 CONTENTS



1.什么是http劫持，DNS劫持为为何物

2.产生的原因

3.造成的危害

4.反劫持实战

5.改善情况



个人中心

优酷首页

频道分类



宫锁连城:爱最深毒最狠

播放: 3.6亿



陕西官员问政现场被免职

播放: 10



[大话]看男友手机不得已

播放: 29.9万



为我推荐



逆向行驶拒罚



舌尖上的中国
A BITE OF CHINA

第二季 心传 心口相传 延续家的味道

共分为《脚步》、《心传》、《时节》、《家常》



原创分享 (1160)

牛男搞笑: 亲宝儿歌[高清版]: 十万个冷幽默



VIP电影 (672)

二龙湖浩哥之风云再起: 澳门风云



全网独播 (4673)

独家电影: Hotel King: 妈妈的庭院



步步惊情: 若曦四爷泪纷纷 (1188)

步步惊情: 步步惊情来丽减版



金玉良缘: 元宝麒麟笑断魂 (987)

搜索

[语音] 下午15:50



下午14:28

上午10:57

凌晨01:45

昨天 晚上

昨天 下午

昨天 中午

昨天 早上 [语音]



微信



通讯录



朋友们



设置

被低俗广告流量劫持后的 微信页面

区别：

被流量劫持的广告与
微信文章间的分割线为
“赞助商链接”等字样，
有“关闭广告”按钮，
且多为低俗广告。→



谁是车坛最有权力的人 陈虹OR陈玉东?

王灿彬 70 23935

2015-05-30

2000多万的年产销规模，中国连续多年成为全球销量最大的市场，中国的汽车人的影响力自然延伸至海外。那么问题就来了，谁是中国汽车界最有权力的人？作为新锐媒体，一猫觉得有义务来回答案这一问题——重磅推出一猫权力榜。



产生的原因

2.广告插码

1.中小运营商节省流量成本，使用缓存技术，制造一个网速“飞快”的假象

3.恶意攻击

怎么劫持的呢？

Google

域名解析请求
(如发出Google.com请求)



DNS服务器

返回错误的IP
(比如返回百度的IP)

Baidu 百度

域名劫持就发生在数据运输的过程中

造成的危害

- 1.应用数据无法更新**
- 2.非法跳转，导致页面数据无法展示**
- 3.弹出广告影响视觉**
- 4.内嵌非法内容影响APP产品形象**

反劫持实战

1.数据合法性校验

2.数据时效性校验

解决方案

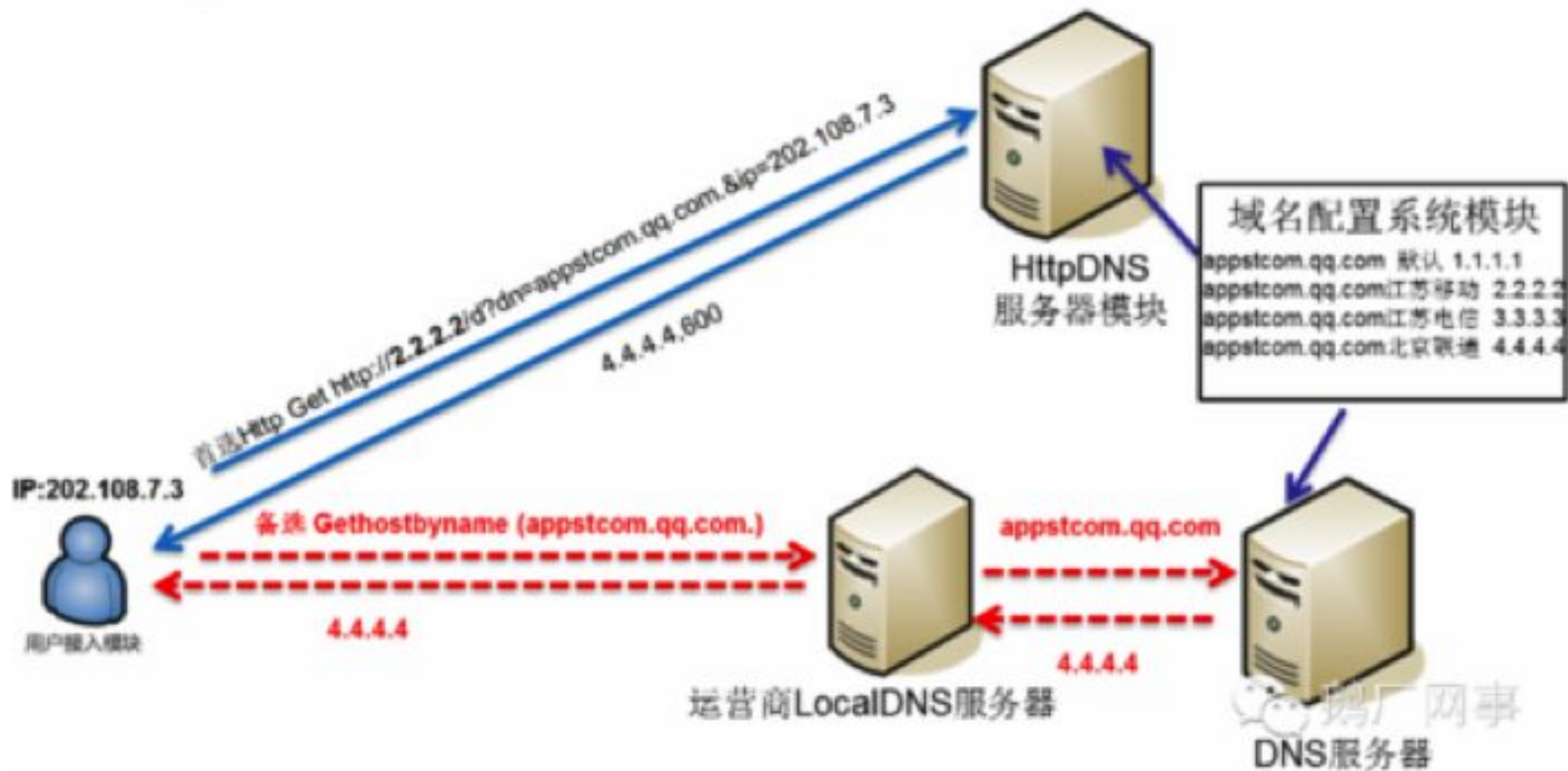
1.域名劫持

2.运营商缓存

3.非法跳转

4.非法内容插入

HttpDNS基本原理

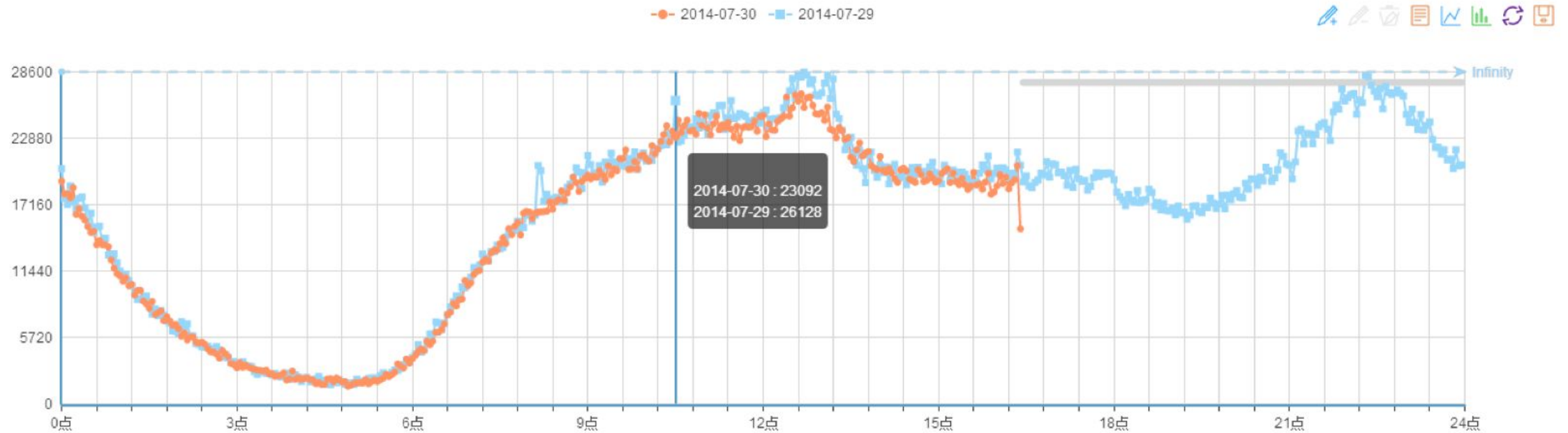


更多

1.网络择优

2.劫持日志系统

实时数据检测：



成功率对比：

月份： 2014-07

当月反劫持数据统计

成功 失败



汽车之家 移动团队 莫松

邮箱：mosong@autohome.com.cn

微信：39151738



Thanks

北京市海淀区丹棱街3号中国电子大厦B座10层 100080

10th Floor Tower B, CEC Plaza, No. 3 Dan Ling Street, Hai Dian District, Beijing 100080, China