刀尖上的舞蹈——DDoS攻防对抗

阿里巴巴集团安全部

朱家睿

DDoS攻击是互联网服务的噩梦，是看不见硝烟的战场

池建强 V

锤子科技云平台研发总监 微博签约自媒体

+ 关注

虽然遭遇了数十G流量的DDoS，但是，官网依约下一轮购买了！牛逼

@池建强 V

购买服务已经恢复，感谢江湖上各位兄弟们的协助，

8月25日 22:32 来自 OS X

8月25日 22:45 来自 Smartisan T1

ipeitimes.com

知乎 V

知乎网官方微博，新浪微博社区委员会专家成员。

+ 关注

【紧急通知】知乎受到外部攻击，导致不可访问，我们正在紧急修复中。请大家先安心工作，我们稍后见。😖

8月5日 17:27 来自 微博 weibo.com

收藏 | 转发 236 | 评论 308 | 422

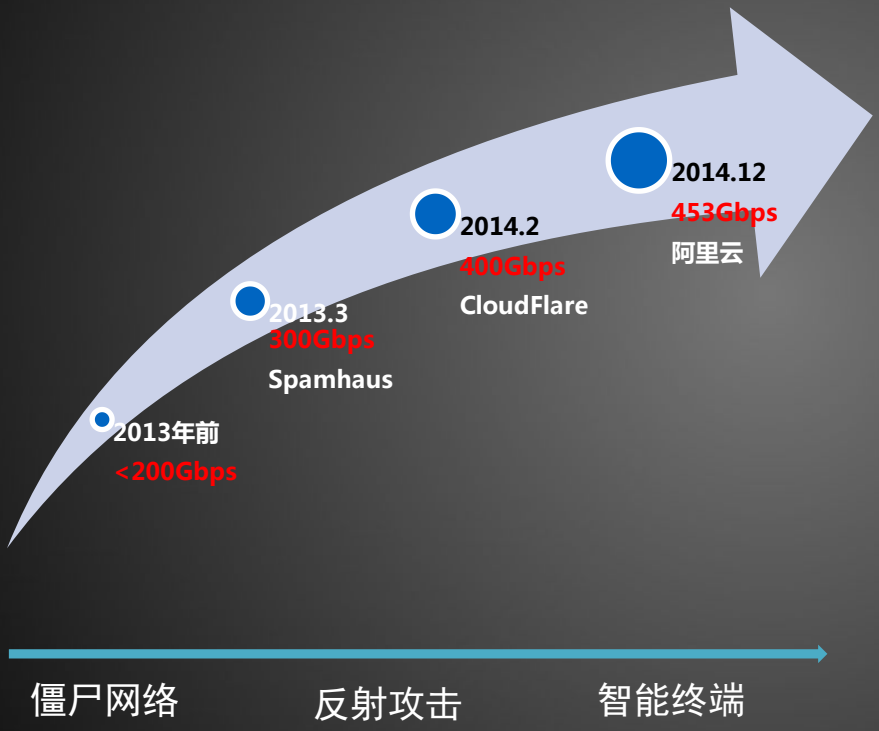
图片来源：新浪微博

什么是 DDoS 攻击 ？

- DDoS（Distributed Denial of Service）
  分布式拒绝服务攻击

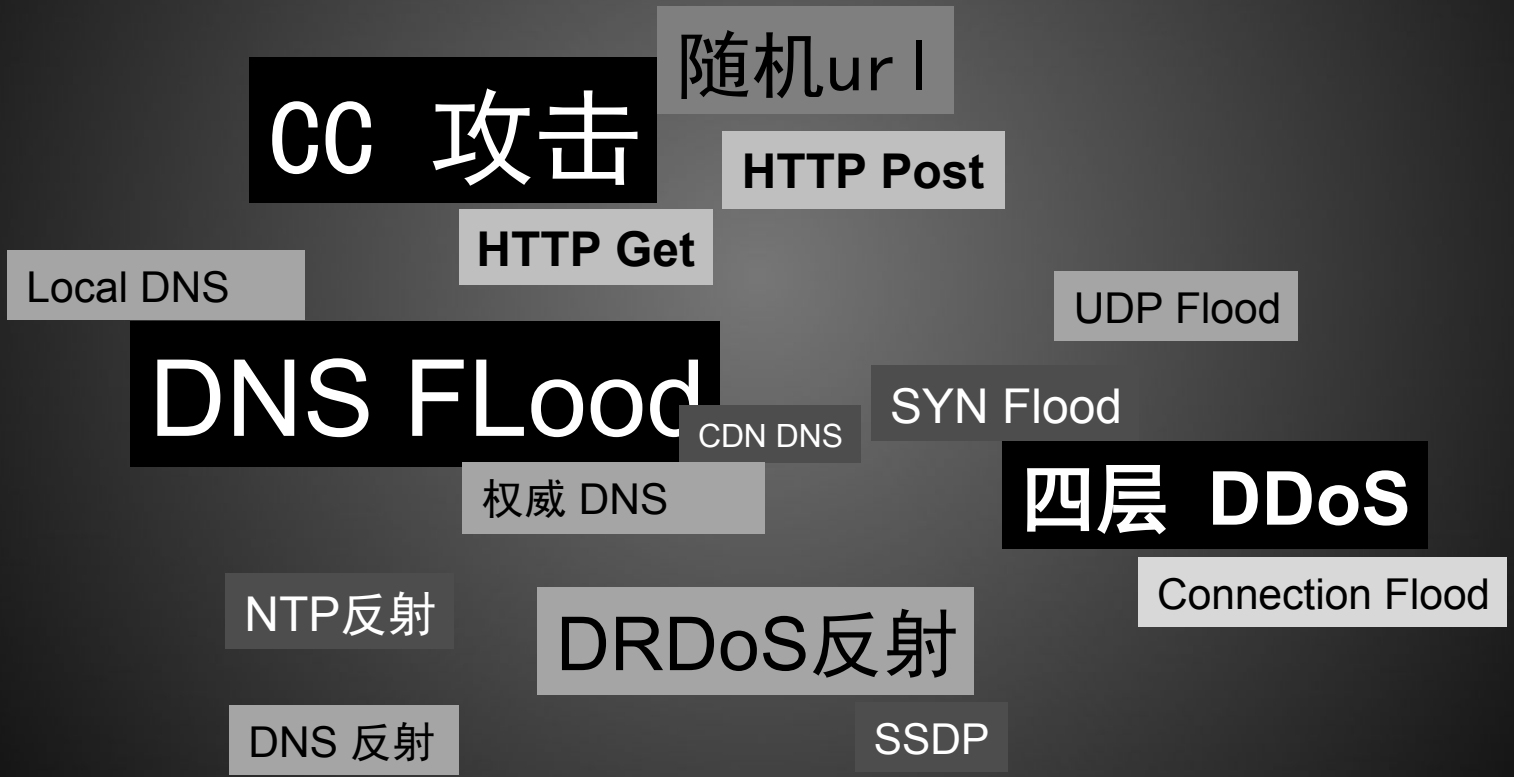
- 堵塞带宽，消耗资源
  让服务器无法提供正常服务

DDoS攻击流量趋势



- DNS、NTP、Chargen反射攻击助力DDoS攻击轻松上百G
- 移动终端也加入“僵尸”网络阵营
- Spamhaus 300G（DNS反射），创造历史
- 阿里云453G，刷新互联网记录！

DDoS攻击不只是大流量



DDoS攻击不只是大流量

随机url

CC 攻击

HTTP Post

HTTP Get

Local DNS

DDoS是力量与巧妙的结合

DNS FLood

SYN Flood

CDN DNS

权威 DNS

四层 DDoS

Connection Flood

NTP反射

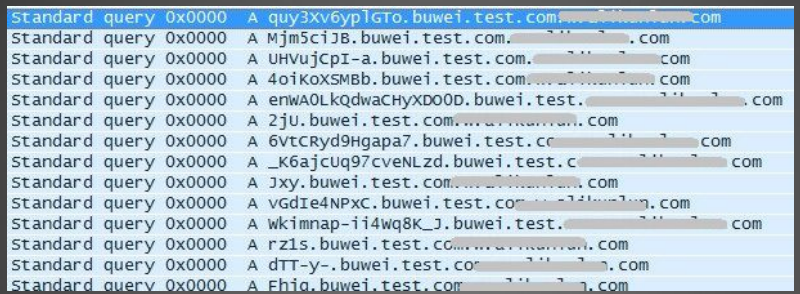
DRDoS反射

DNS 反射

SSDP

几个例子

- 随机域名攻击,Local DNS 无法缓存，权威DNS被打死



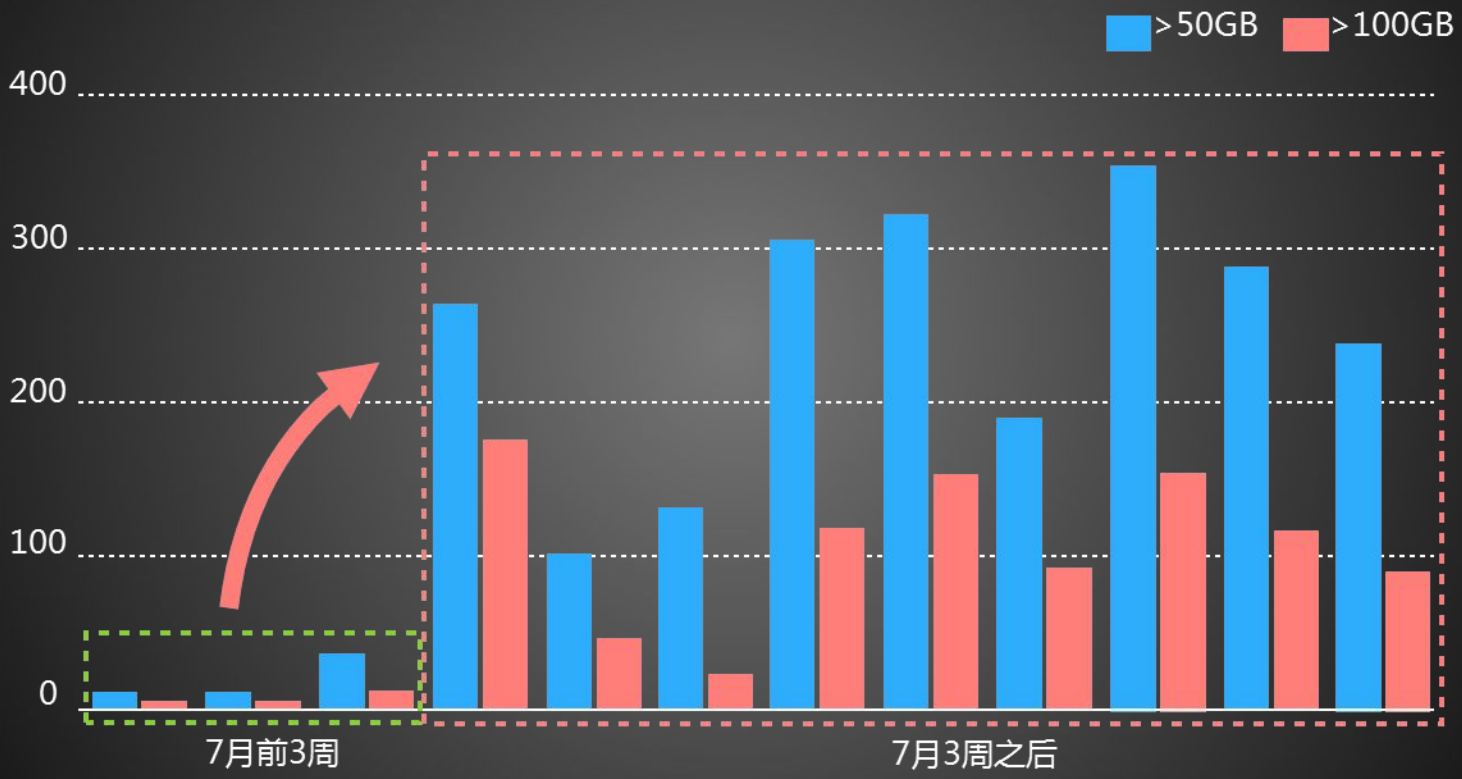
- 随机URL攻击，穿透CDN Cache，源站被打死

URL拦截TOP

URI	拦截次数
/	1285270139
/o.jsp	43251
/p.htm	42787
/k.bmp	42772
/i.gif	42730
/h.jsp	42716
/k.gif	42700
/m.jpg	42697
/u.asp	42691

阿里云云盾
第三季度DDoS态势报告

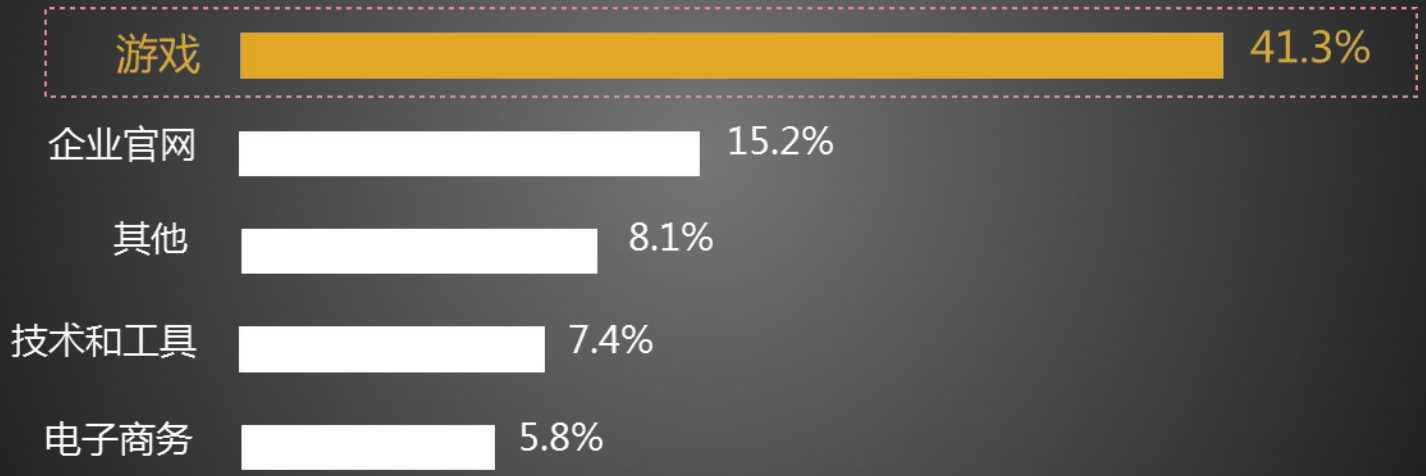
大流量攻击成为常态



详细报告，可关注“阿里云安全”微博、微信获取

哪些行业易被攻击？

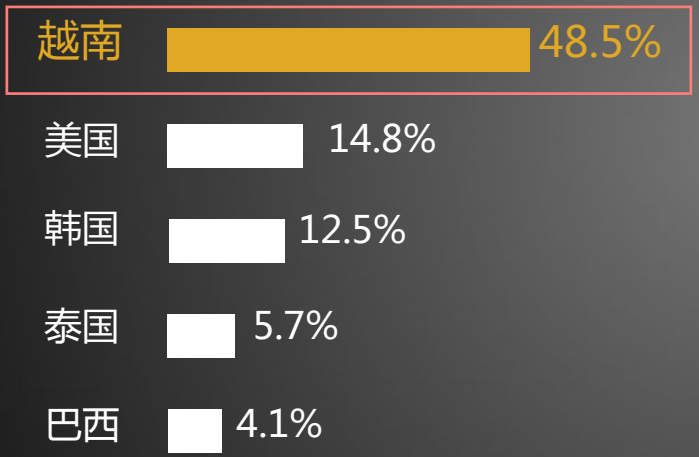
TOP5被攻击行业



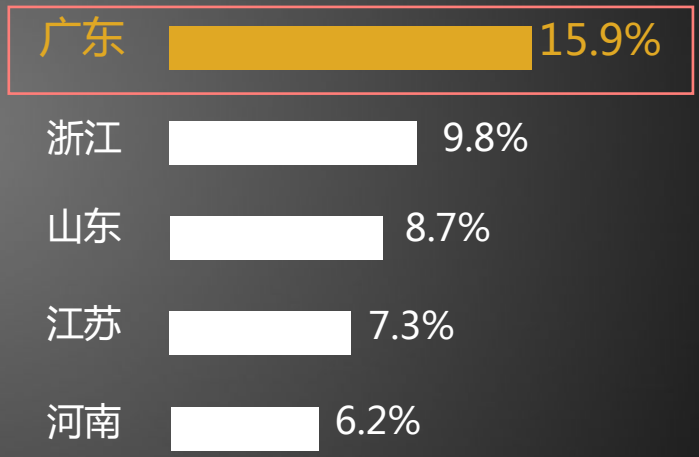
详细报告，可关注“阿里云安全”微博、微信获取

攻击源最多为越南和广东

TOP5国外攻击源



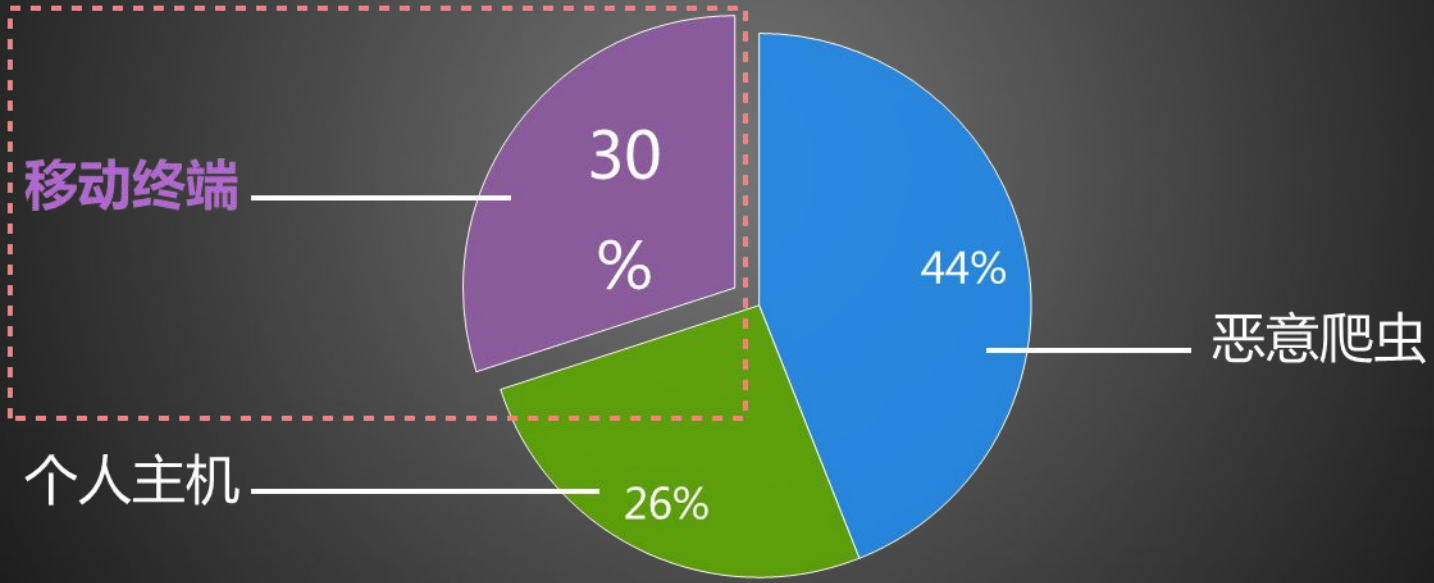
TOP5国内攻击源



详细报告，可关注“阿里云安全”微博、微信获取

移动终端成为新的攻击源

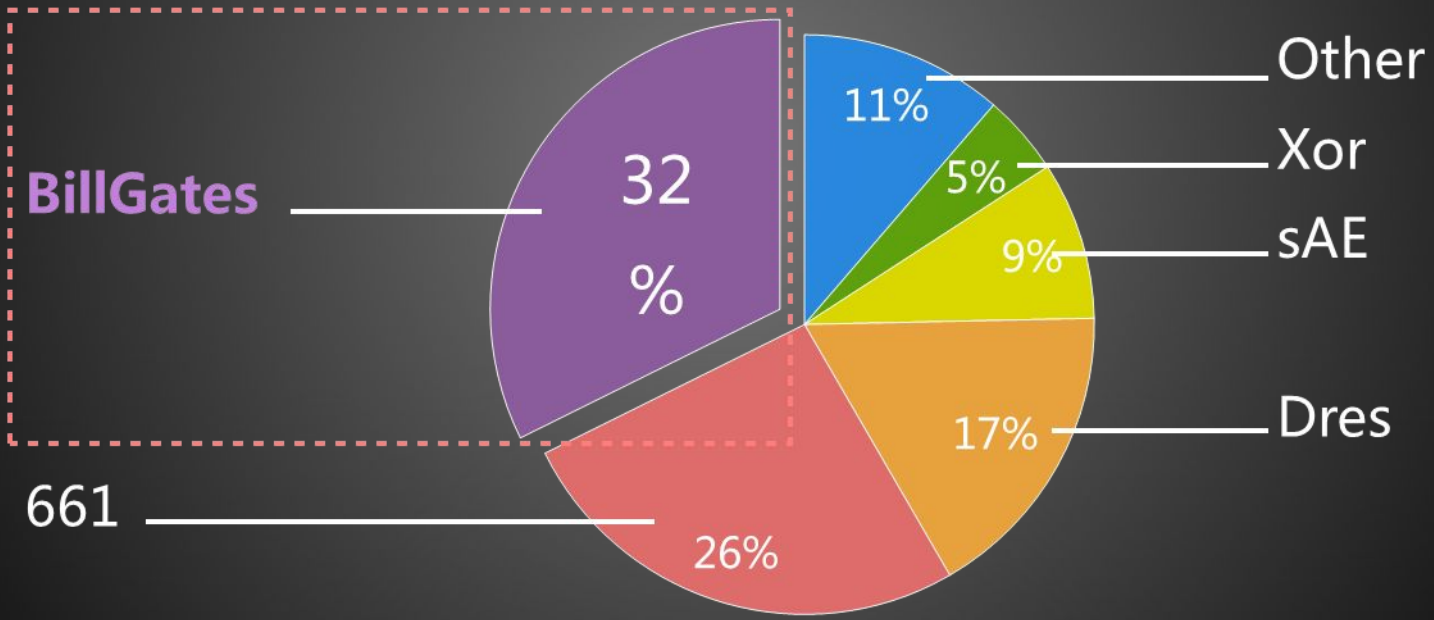
DDoS攻击来源



详细报告，可关注“阿里云安全”微博、微信获取

最活跃的僵尸程序是BillGates

TOP活跃僵尸程序



详细报告，可关注“阿里云安全”微博、微信获取

阿里如何防御？

阿里巴巴众多业务：

天猫、淘宝、支付宝……

CDN 和 云业务

云业务带来的变化：

攻击数量和流量指数级上升

100个用户100种应用，用什么策略？

1Gb/s的正常业务和100Mb/s的攻击如何分辨？

大流量的连带“躺枪”

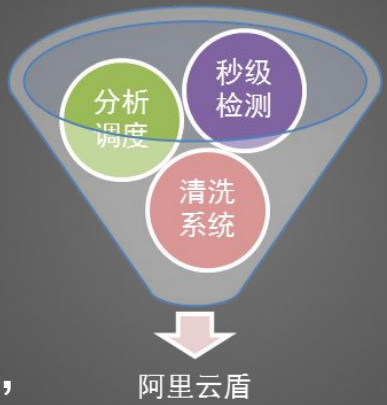
……

自主研发

- 自主研发，贴合业务，模块间紧密配合
- 快速迭代，适应业务发展

分析调度

- IP业务识别和策略自学习
- 大数据分析，10万种业务，1千种模型



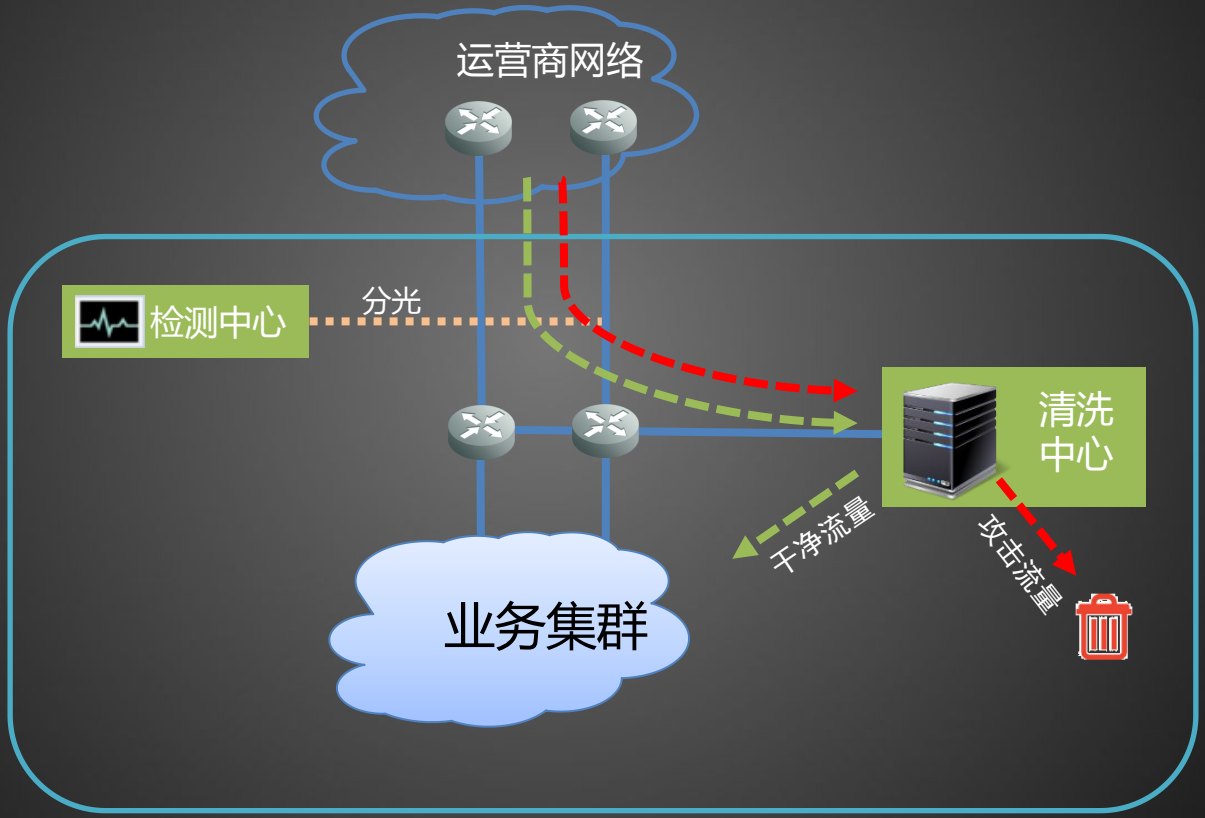
秒级检测

- 分光检测，1S级预警，2秒完成处理，避免躺枪
- 20种流量成分秒级判断，精确判断攻击
- 流量阈值自学习

清洗系统

- 高性能：单台百G
- 线性扩容，TB容量
- 四到七层全面防御

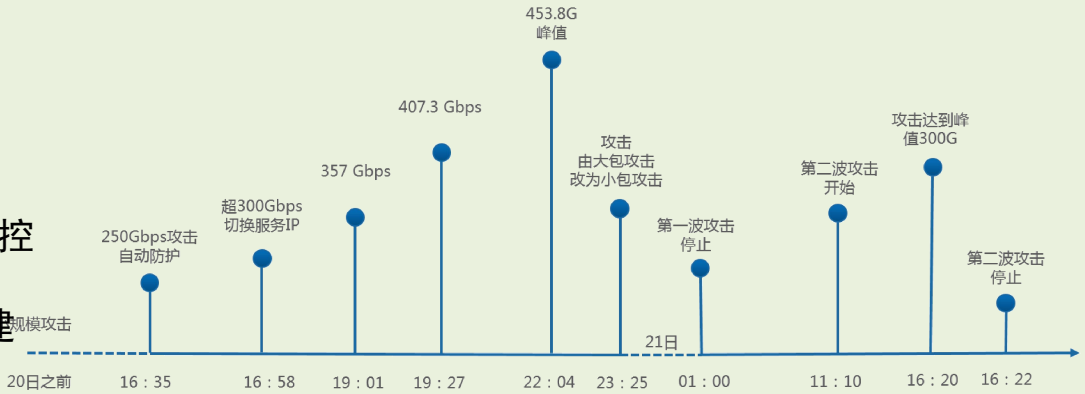
部署逻辑



防御案例分享

453.8G DDoS 攻击事件

- 带宽储备+ABTN
- 攻击监控
- TB级清洗容量
- ISP各方向链路状态监控
- 防御预案
- 攻击源分析，为防御建设提供数据



防御案例分享

“毫发无损的发布会”

- 攻击最大40G
- 发布会1秒都没有受影响
- 预案做在前面

DDoS防御是一项系统工程

事前，充分准备

事中，快速响应

事后，加强总结

事前

- 监控：全面、快速、准确的“看清楚”威胁

- 强身健体：能力建设

- 体检：定期的攻防演练

- 预案：不打无准备之仗

事中

- 分析攻击，见招拆招
- 团队配合，分工联动
- 流程打磨，快速处理
- 攻防经验，有条不紊

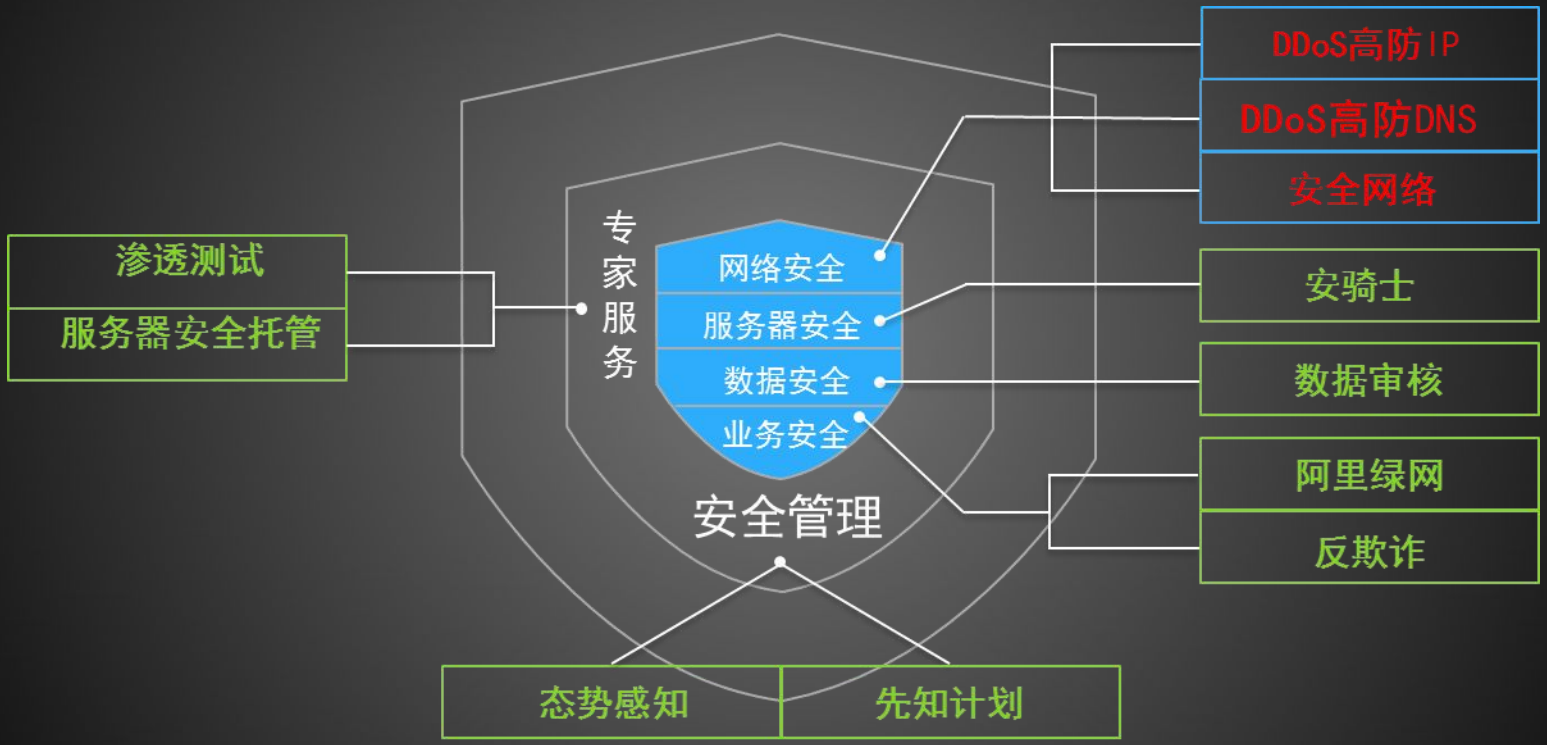
事后

- 分析Review，找出薄弱环节，为下一次战役做准备

我们熟悉的木桶原理

- 薄弱的地方，往往造成最大的破坏

全面防护不留死角


DDoS高防IP
DDoS高防DNS
安全网络
渗透测试
服务器安全托管
专家服务
网络安全
服务器安全
数据安全
业务安全
安骑士
数据审核
阿里绿网
反欺诈
安全管理
态势感知
先知计划

中小企业的DDoS难题

中小企业的DDoS难题

- 买一堆的安全设备是否能解DDoS?
- 带宽军备竞赛？小企业买400G带宽？
- 培养一支7*24小时的专家团队？
- 真正被攻击了，设备、人、流程的反应时间有多快？

我们的答案是

云端防护

云计算重新定义DDoS防护

- 安全托管，回归业务
- 弹性的安全防护
- 云端海量带宽
- 云上的运维专家
- 大数据下的防御

但是，
问题依然存在

DDoS防御的痛点

1 军备竞赛
性价比低

3 单点风险

2 带宽扩容
还能走多远？

4 线路质量不够高

如果可以做到：

1 摆脱军备竞赛

3 风险分散

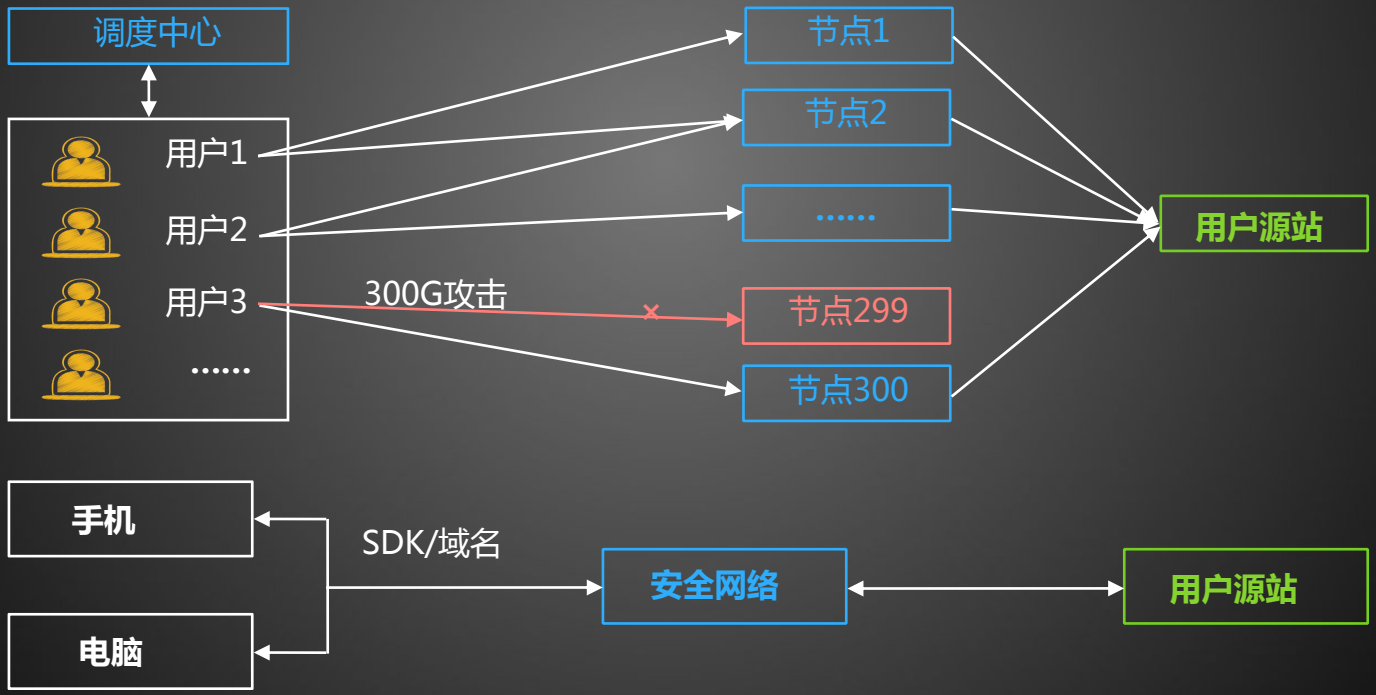
2 防护模式与业务的完美结合

4 优质多线路接入近源访问

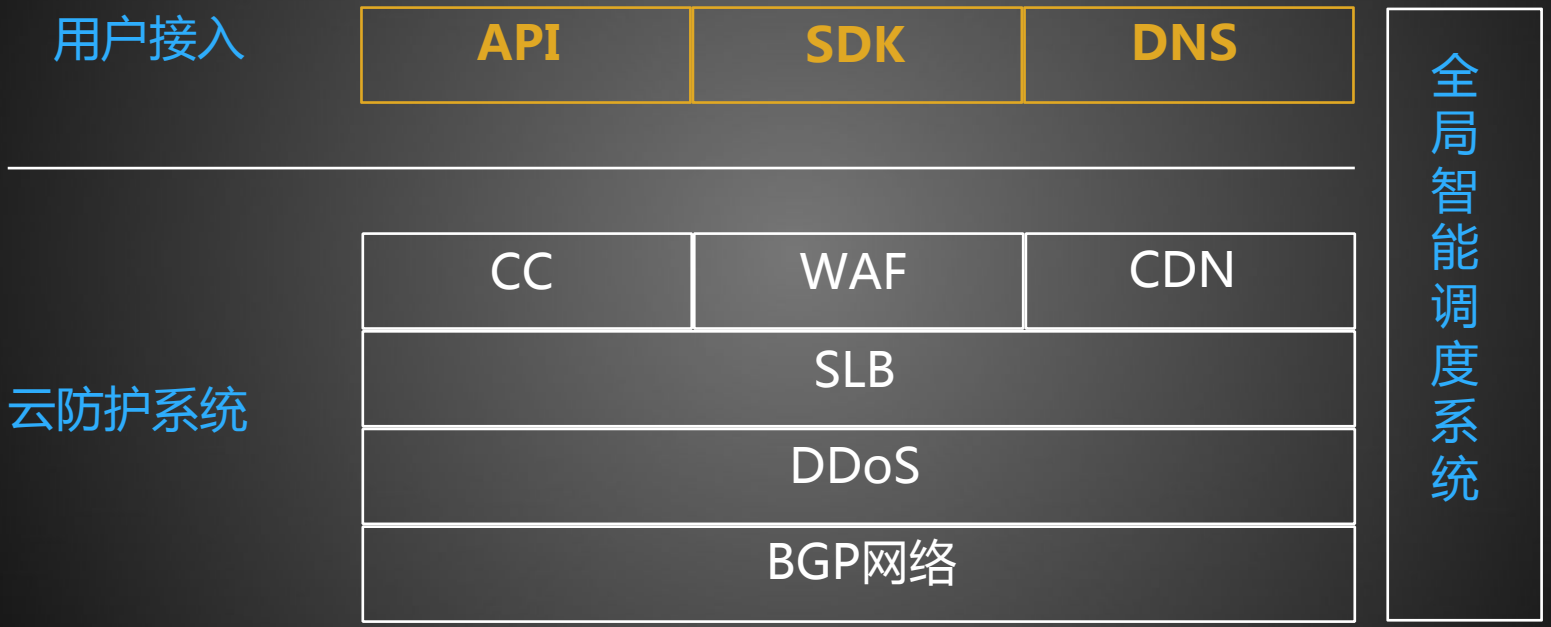
我们的新思路

安全网络

一种安全可靠的**接入**网络**服务**。
通过安全网络节点（IP），为源站提供安全、稳定、快速的流量。



全面立体的接入体系



Thanks

更多安全资讯

微博：阿里云　阿里云安全

微信公共号：阿里云　阿里云安全

http://www.aliyun.com/product/esn