

刀尖上的舞蹈——DDoS攻防对抗

阿里巴巴集团安全部

朱家睿

Geekbang>

极客邦科技

全球领先的技术人学习和交流平台

扫我，码上开启新世界



Geekbang>

InfoQ | EGO NETWORKS | StuQ

InfoQ

专注中高端技术
人员的社区媒体

EGO

EXTRA GEEKS' ORGANIZATION

NETWORKS

高端技术人员
学习型社交网络

StuQ

实践驱动的IT职业
学习和服务平台



促进软件开发领域知识与创新的传播



实践第一 案例为主

时间：2015年12月18-19日 / 地点：北京·国际会议中心

欢迎您参加ArchSummit北京2015，技术因你而不同



ArchSummit北京二维码



【北京站】

2016年04月21日-23日



关注InfoQ官方信息
及时获取QCon演讲视频信息

DDoS攻击是互联网服务的噩梦，是
看不见硝烟的战场



池建强  

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  

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



知乎 

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

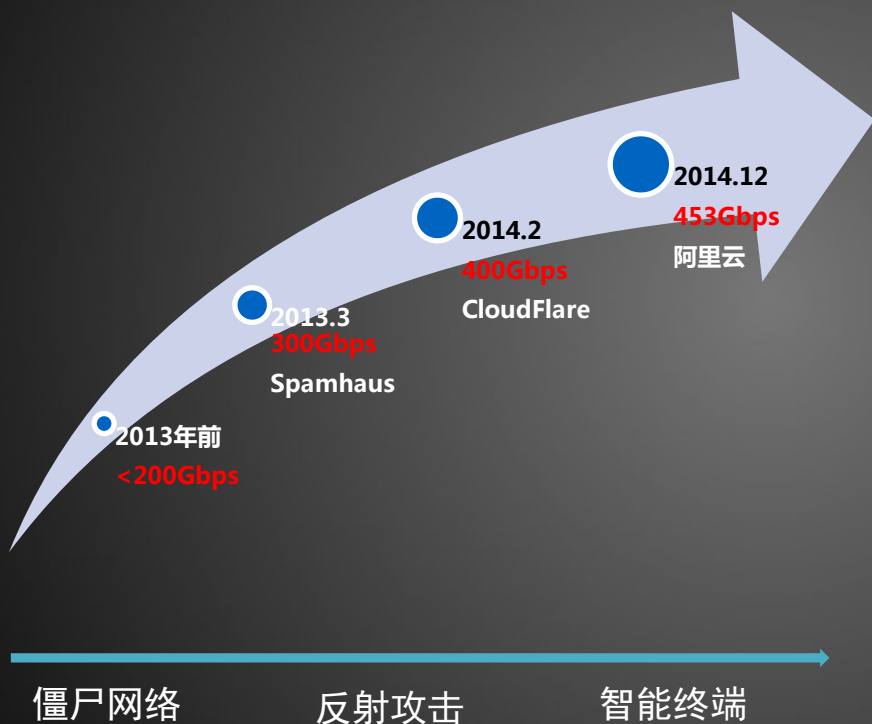
图片来源：新浪微博

ipeitimes.com

什么是 DDoS 攻击？



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

CC 攻击

随机url

HTTP Post

HTTP Get

Local DNS

UDP Flood

DNS Flood

CDN DNS

SYN Flood

权威 DNS

四层 DDoS

Connection Flood

NTP反射

DRDoS反射

DNS 反射

SSDP

DDoS攻击不只是大流量

CC 攻击

随机url

HTTP Post

Local DNS

DDoS是力量与巧妙的结合

DNS Flood

SYN Flood

权威 DNS

CDN DNS

四层 DDoS

NTP反射

DRDoS反射

Connection Flood

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

```
Standard query 0x0000 A quy3Xv6yp1GTo.buwei.test.com.
Standard query 0x0000 A Mjm5ciJB.buwei.test.com.
Standard query 0x0000 A UHVujCpI-a.buwei.test.com.
Standard query 0x0000 A 4oiKoxSMBb.buwei.test.com.
Standard query 0x0000 A enWA0LkQdwaChyXD00D.buwei.test.com.
Standard query 0x0000 A 2jU.buwei.test.com.
Standard query 0x0000 A 6vtCRyd9Hgapa7.buwei.test.com.
Standard query 0x0000 A _K6ajcuq97cveNLzd.buwei.test.com.
Standard query 0x0000 A Jxy.buwei.test.com.
Standard query 0x0000 A vGdIe4NPxC.buwei.test.com.
Standard query 0x0000 A wkimnap-ii4wq8K_J.buwei.test.com.
Standard query 0x0000 A rz1s.buwei.test.com.
Standard query 0x0000 A dTT-y-.buwei.test.com.
Standard query 0x0000 A Fhiq.buwei.test.com.
```

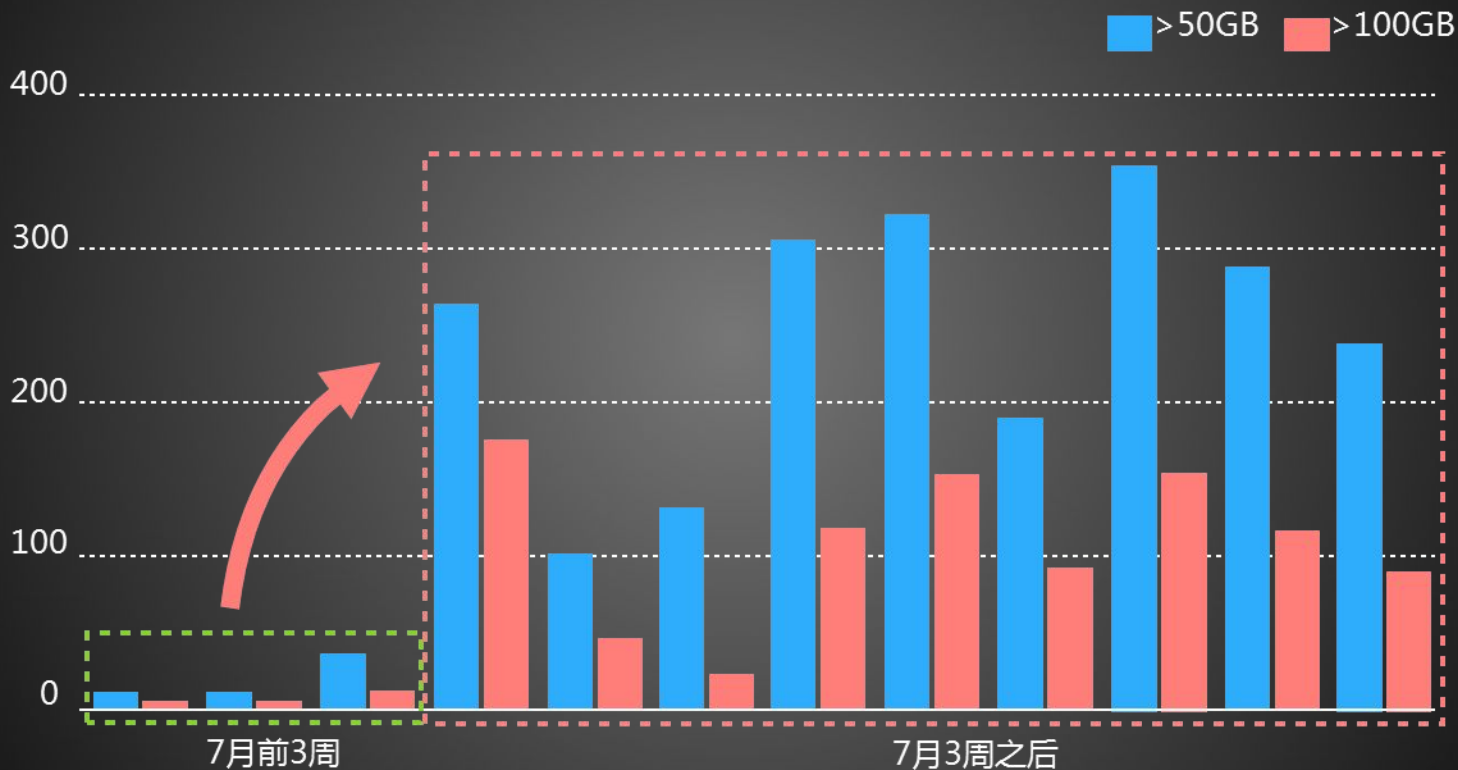
- 随机URL攻击, 穿透CDN Cache, 源站被打死

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

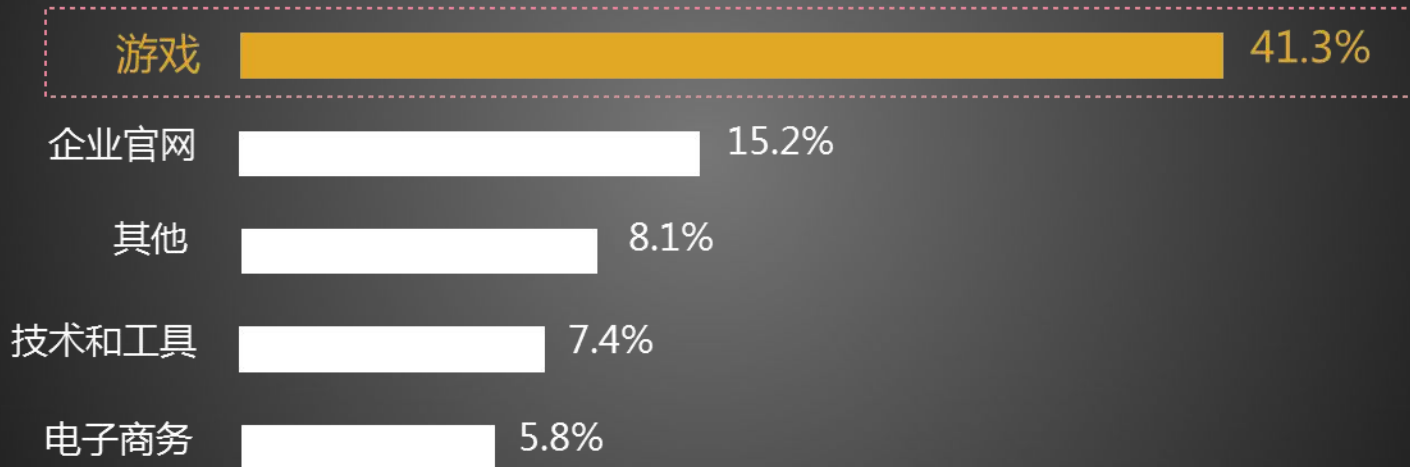
大流量攻击成为常态



详细报告，可关注“阿里云安全”微博、微信获取

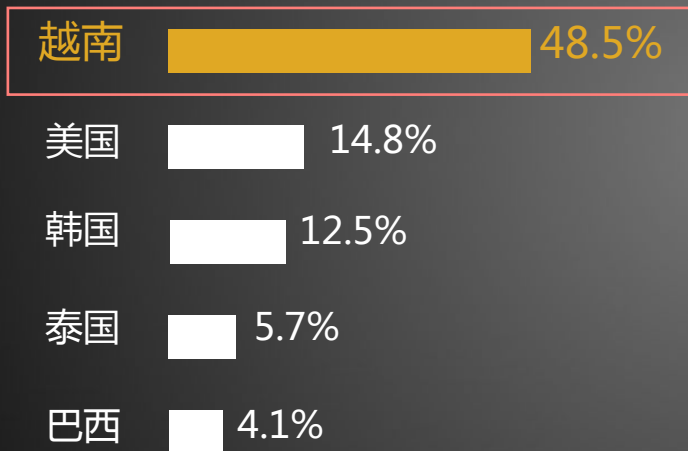
哪些行业易被攻击？

| TOP5被攻击行业

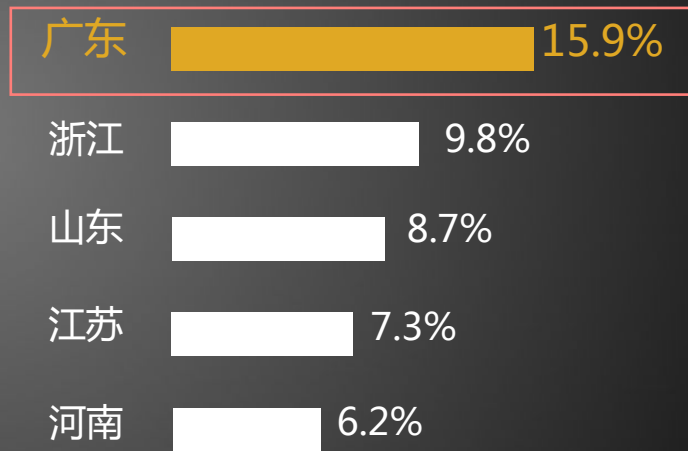


攻击源最多为越南和广东

| TOP5国外攻击源

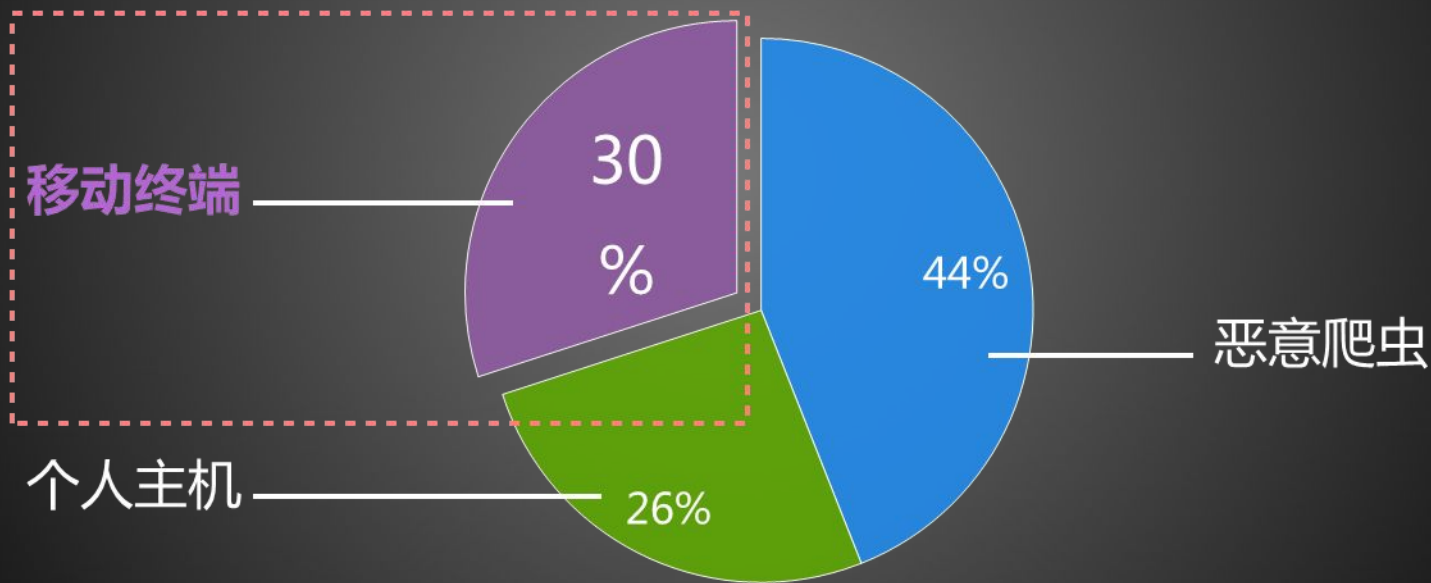


| TOP5国内攻击源



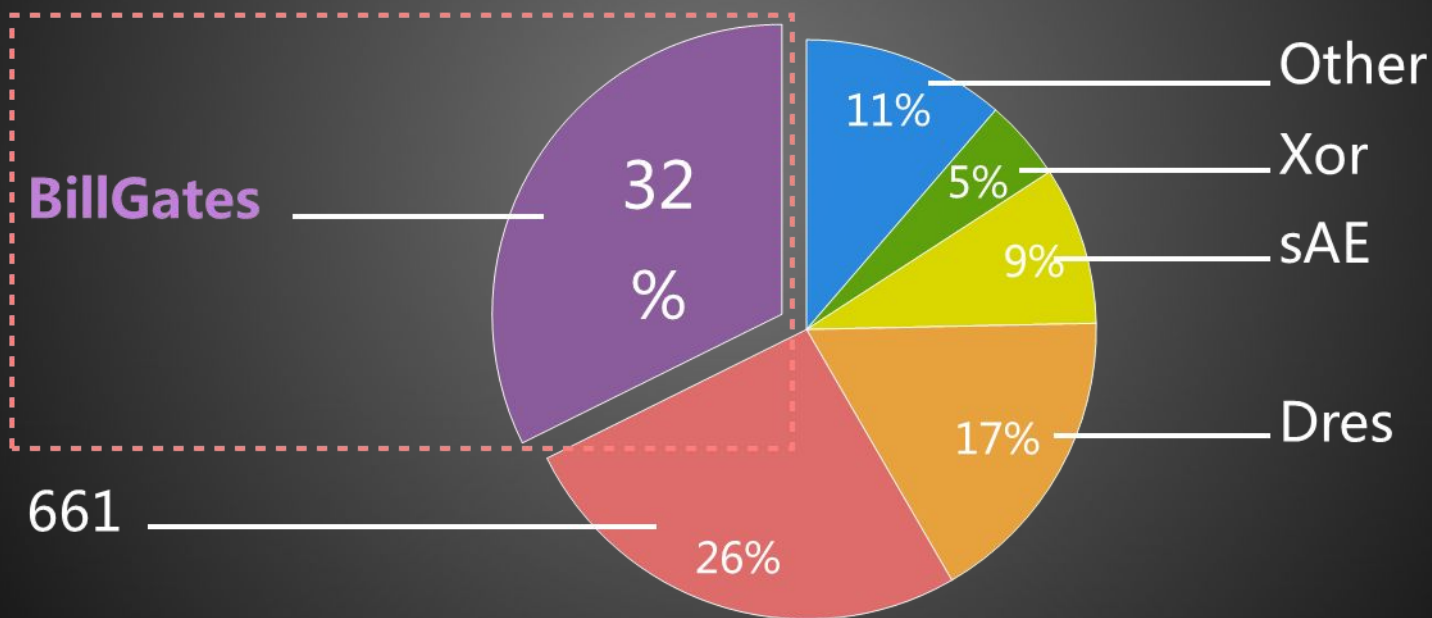
移动终端成为新的攻击源

| DDoS攻击来源



最活跃的僵尸程序是Bill Gates

TOP活跃僵尸程序



阿里如何防禦？

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

秒级检测

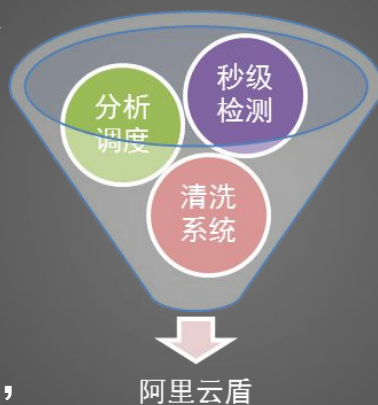
- 分光检测，1S级预警，2秒完成处理，避免躺枪
- 20种流量成分秒级判断，精确判断攻击
- 流量阈值自主学习

分析调度

- IP业务识别和策略自主学习
- 大数据分析，10万种业务，1千种模型

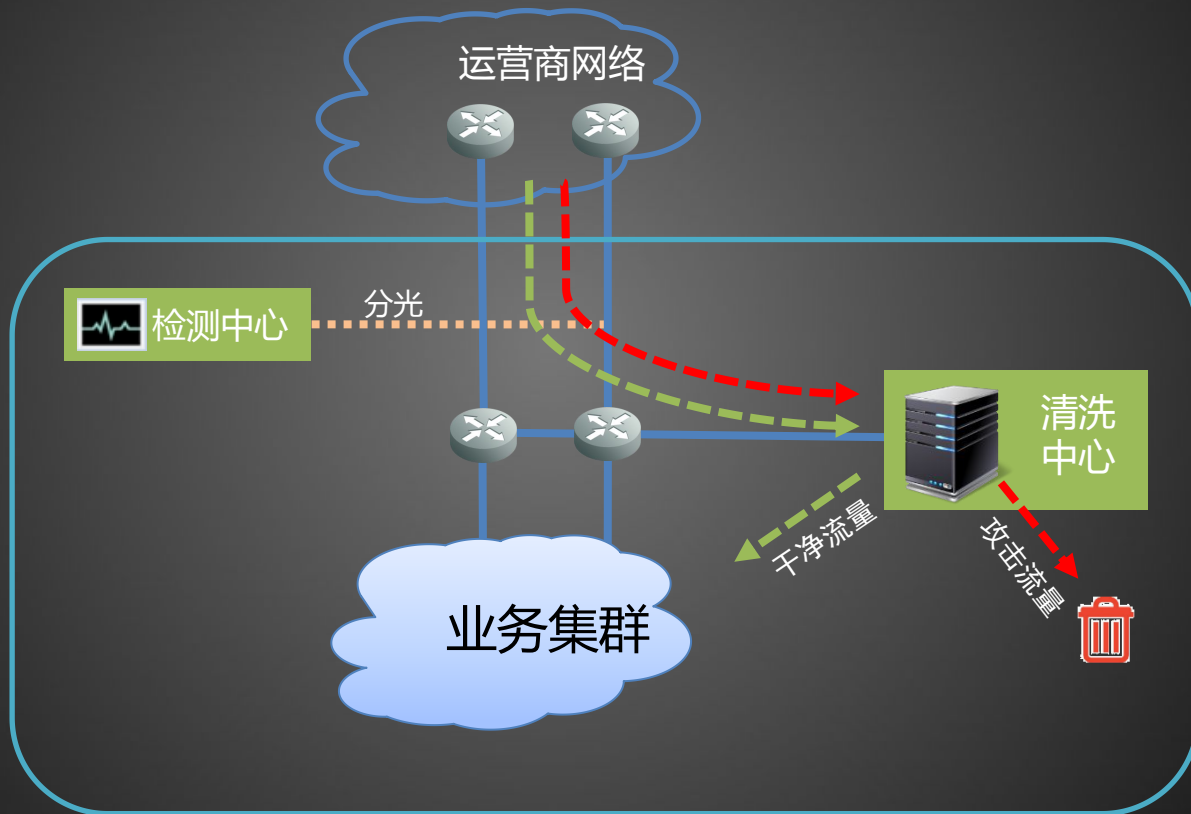
清洗系统

- 高性能：单台百G
- 线性扩容，TB容量
- 四到七层全面防御



阿里云盾

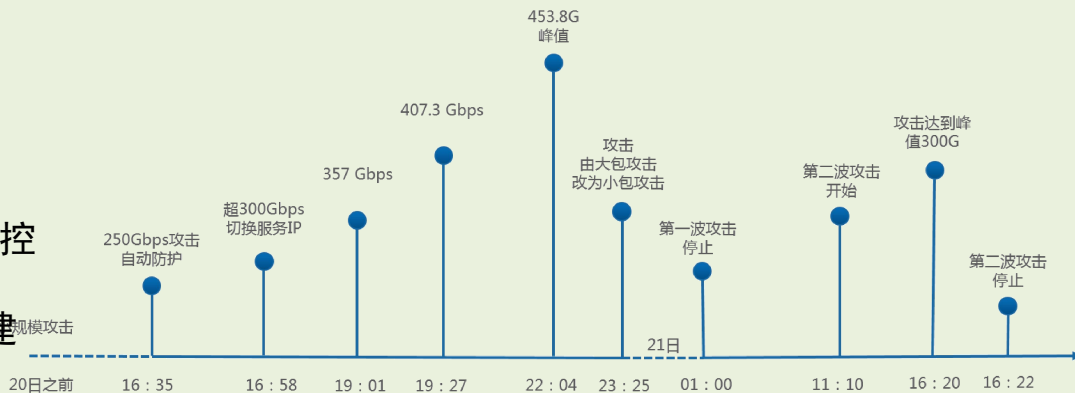
部署逻辑



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

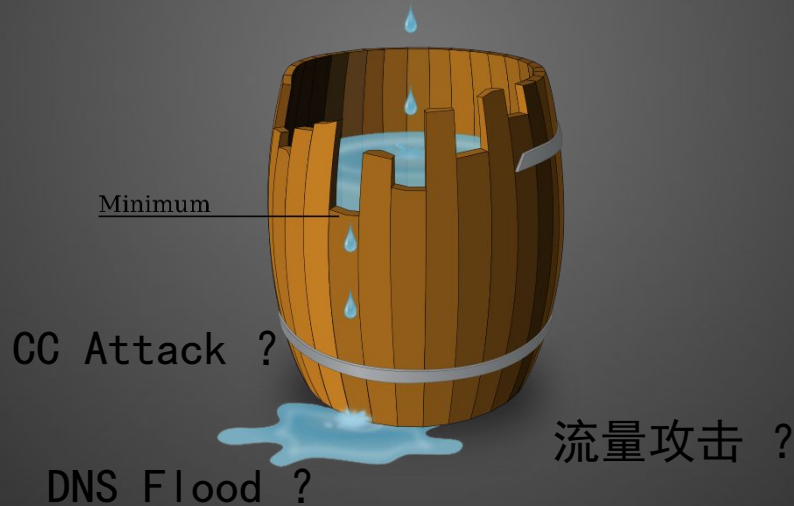
事后



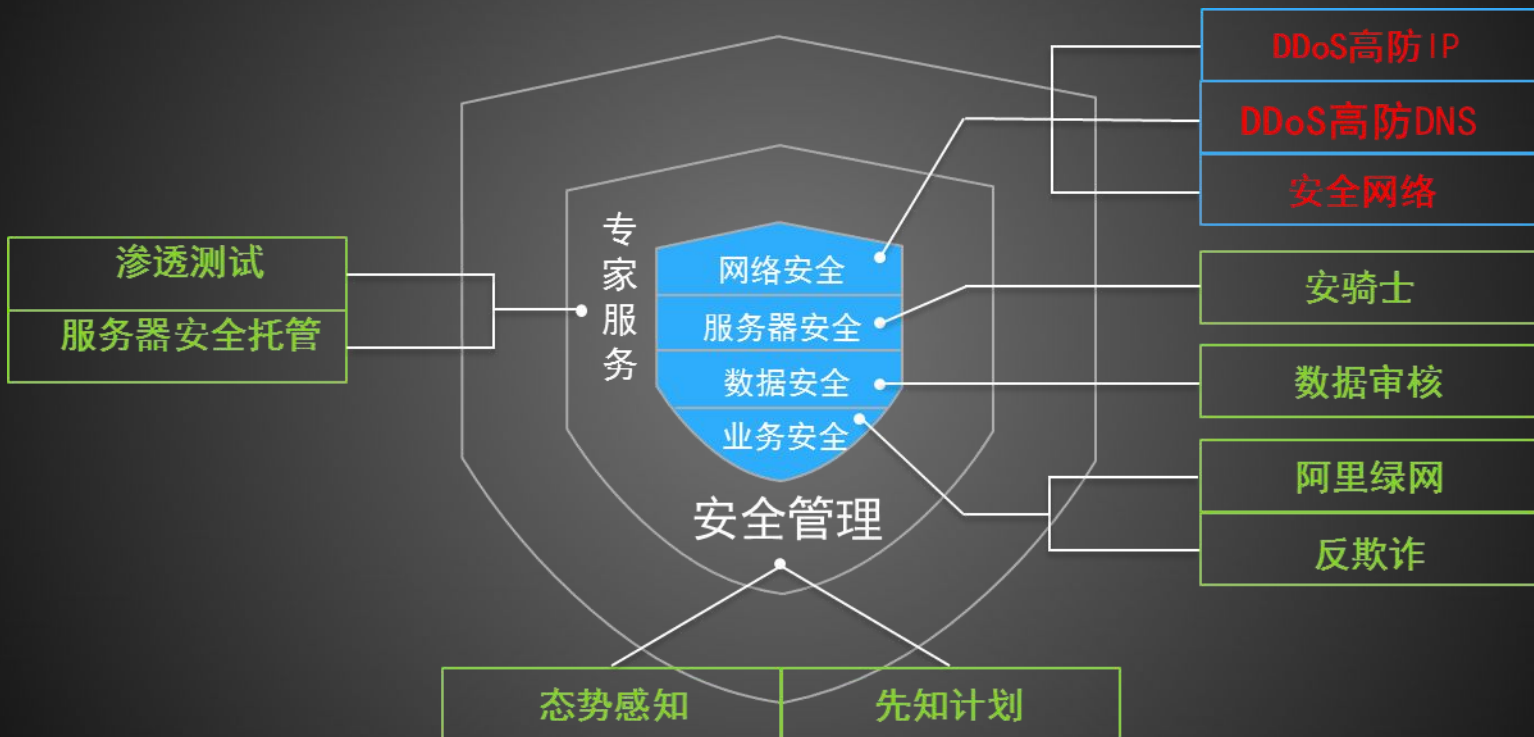
- 分析Review，找出薄弱环节，为下一次战役做准备

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



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

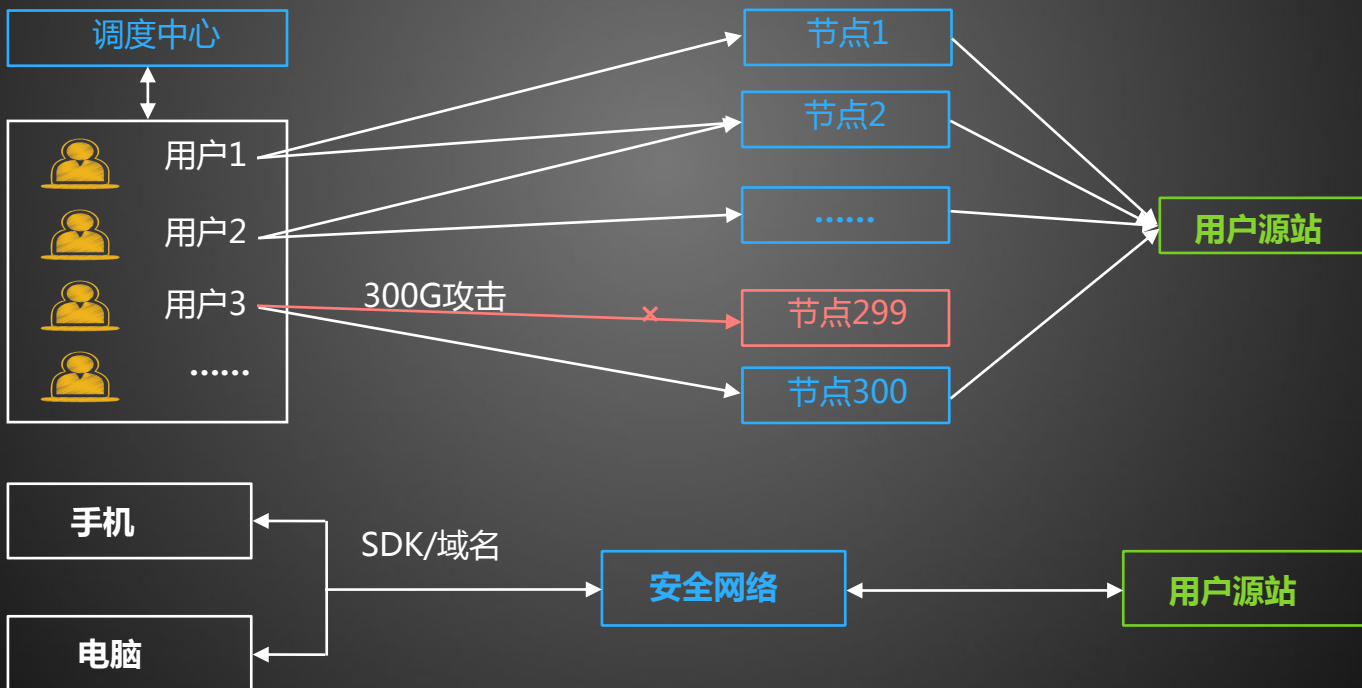
**4 优质多线路接入
近源访问**

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

用户接入

API	SDK	DNS
-----	-----	-----

全局智能调度系统

云防护系统

CC	WAF	CDN
SLB		
DDoS		
BGP网络		

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>

