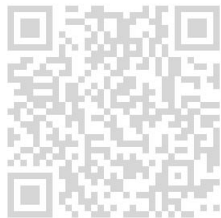


基础网络运营商的网络能力开放实践

刘紫干
中国电信集团

中国系统架构师大会 SACC2019
北京· 2019.11.01



全新IT技术私域交流平台

什么是基础网络运营商

- 能够不依附于第三方、自己独立构建并运营泛在的端到端基础网络通达能力的实体
- Underlay VS. Overlay
- 在我国，从内涵看，“通信” > “电信” > “基础网络”

什么是网络能力

- 是**按需的、动态的**使用**网络资源**的能力
- 打破长久的误区，网络资源 \neq 网络能力

我对网络资源的理解

硬资源

设备、线路、机房、铁塔...

软资源

流量、数据、协议、架构...

网络资源

这里才是“力量”所在

看摊

目标：“独善其身”
过程：守好，别出事儿

硬资源
+
软资源

赋能

目标：“兼济天下”
过程：用好，多整事儿

中国电信作为我国互联网基础资源的主要建设者和拥有者，
在网络安全领域，需要同时做到**守土有责**、**积极赋能**，挑战巨大！



有时候

看似复杂的问题可以用简单的方式解决

只要你

位置对，视角好，有资源，敢架构

运营商如果进入网络安全服务领域，

做什么事情可能有戏？

$$E = c * \max \{f(\text{位置}, \text{视角}, \text{资源}, \text{架构})\}$$

E – 能力开放效果， c – 痛点系数， f – 禀赋函数

网络安全服务的痛点中，哪些问题运营商可能有机会？

界线 → 责任 → 可控范围



域内可控，但域外不可控！

典型的不可控的从“围墙”外产生的安全威胁

- DDoS攻击
- DNS安全威胁
- 仿冒欺诈
- 路由安全（也许SDN能解决一部分问题）

安全的核心是风险可控，就是变“不可控”为“可控”的过程

靠自身力量就可控 + 要借助外力才可控

业务的载体 — 互联网络（恶意攻击，路由稳定，域名解析正确，站点仿冒...）

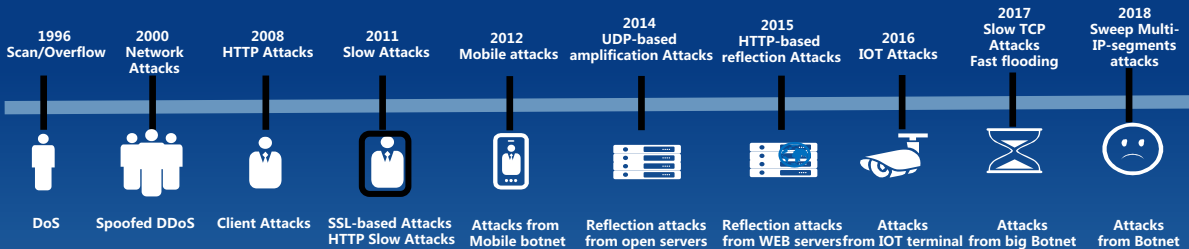
业务的场景 — 移动化/虚拟化（Web安全，访问身份的鉴别，交易异常的多因素判断...）

DDoS攻击

DDoS攻击的实质

- DDoS攻击限于资源消耗型的攻击
 - 带宽资源
 - 计算资源 (系统、应用)
- DDoS攻击都是在“局部”造成压倒性资源消耗

DDoS攻击技术演变趋势



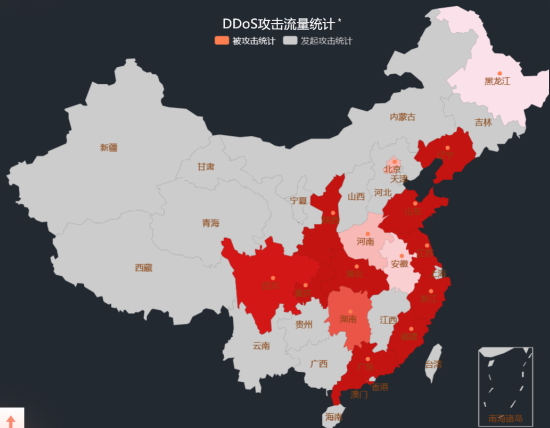
全国范围

目标

源

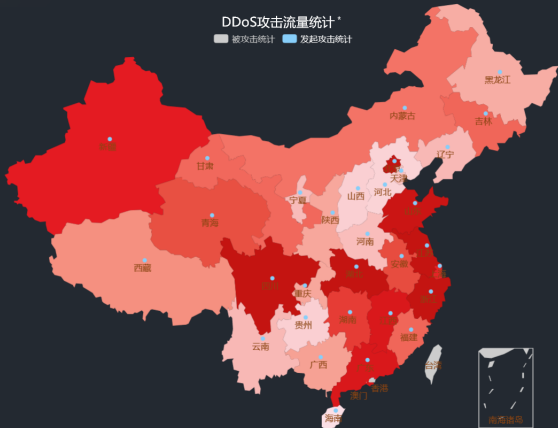
DDoS攻击流量统计*

被攻击统计 发起攻击统计



DDoS攻击流量统计*

被攻击统计 发起攻击统计



我国DDoS攻击整体趋势

聚焦2019年5月

46000TByte (~142Gbps)

0.88Tbps 攻击峰值

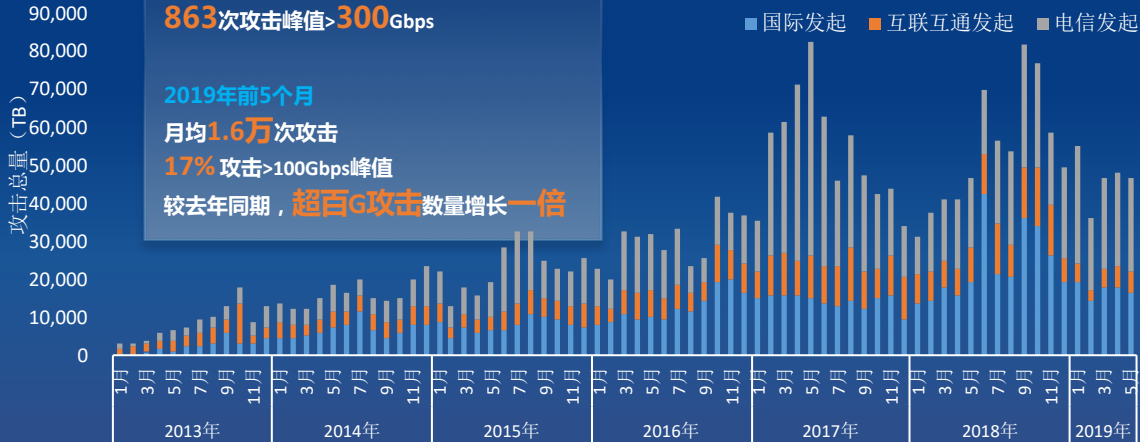
863次攻击峰值>300Gbps

2019年前5个月

月均1.6万次攻击

17% 攻击>100Gbps峰值

较去年同期，超百G攻击数量增长一倍



数据源：电信云堤 <http://www.damddos.com/networkattack.html#page3>)

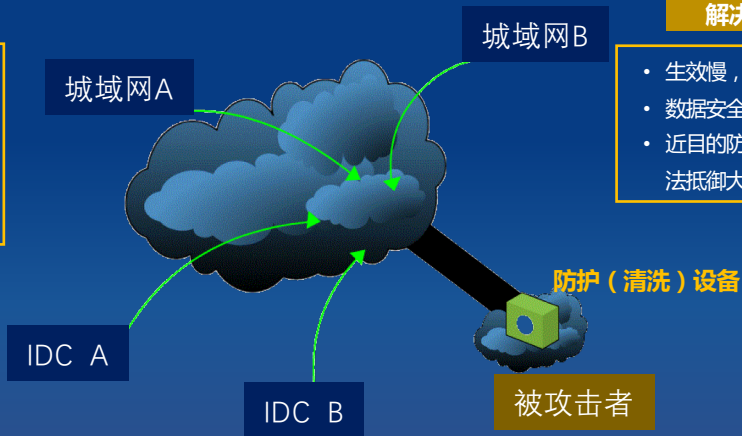
传统解决方案无法有效防护DDoS攻击

客户自防护

- 无法对攻击流量大小进行监控
- 近目的防护，无法解决接入带宽拥塞
- 没有专业团队运营

互联网厂商解决方案

- 生效慢，需变更IP
- 数据安全性无法得到保障
- 近目的防护，时延大，无法抵御大流量攻击



云堤的近源防护能力

某客户遭受DDoS攻击



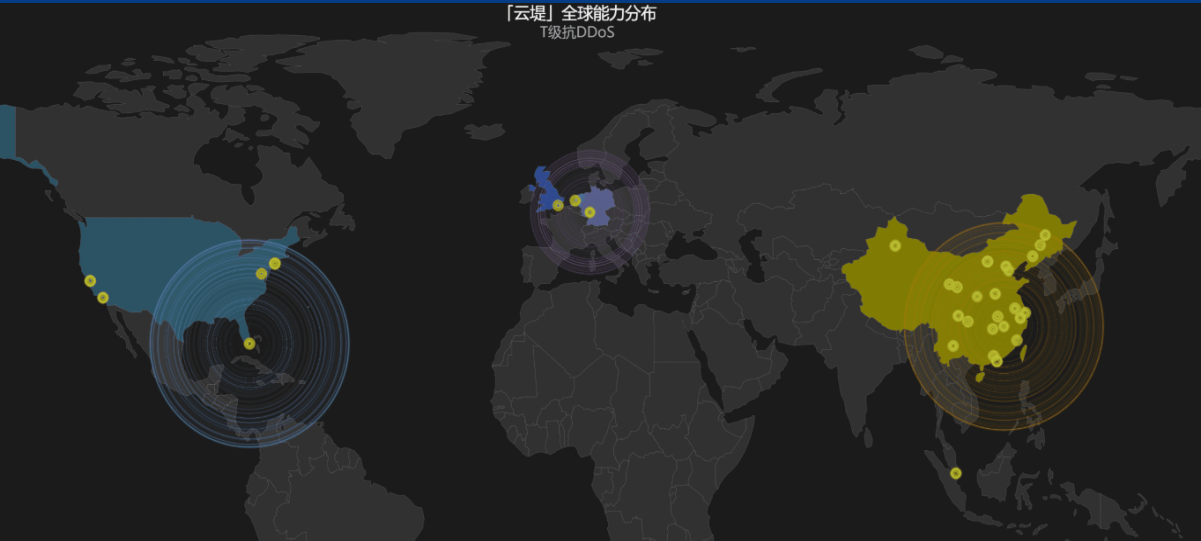
近目的防护

云堤启动，近源清洗

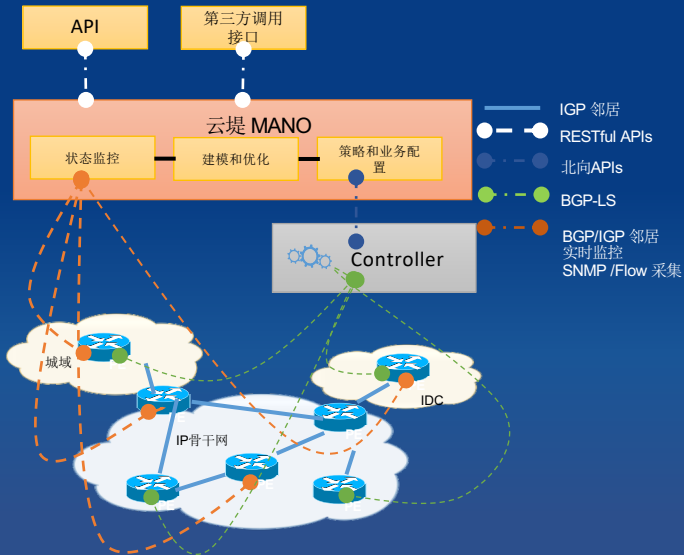


分布式近源防护

「云堤」全球能力分布
T级抗DDoS



对骨干网进行业务调度的SDN架构



- **云化**：云堤的控制运营平台在2016年11月底全部云化改造完毕
- **微服务化**：将流量压制、重定向、清洗调度等路由控制速度从之前的分钟级提升到2秒以内，从串行到支持高并发
- **标准化**：资源纳入统一的控制器服务网关进行管理，内部实现统一的Restful接口标准，
- **异地双活化**：控制器层面实现容灾转移能力

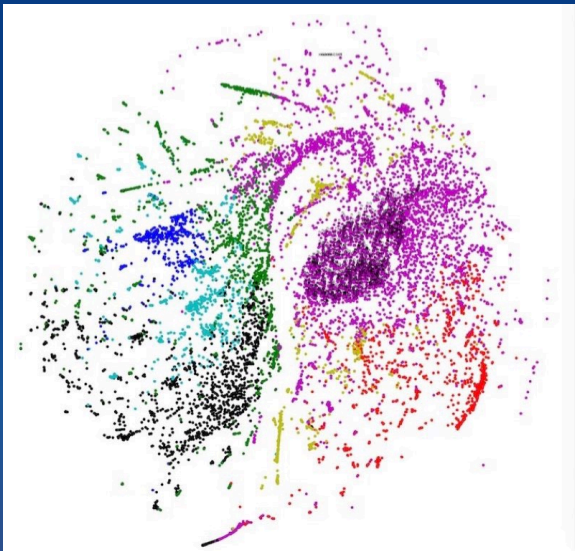
防得住 — 路由的控制能力，即是防守资源的调度能力

- 分方向的流量压制
 - 国际、国内互联互通、仅电信网内、省域/IDC出口
 - 实现：RTBH、FlowSpec、RR+
- 攻击流量的牵引清洗
 - BGP到IGP的迭代
 - “指哪牵引到哪”
 - 散落各地的带宽资源为一次防御所集中利用

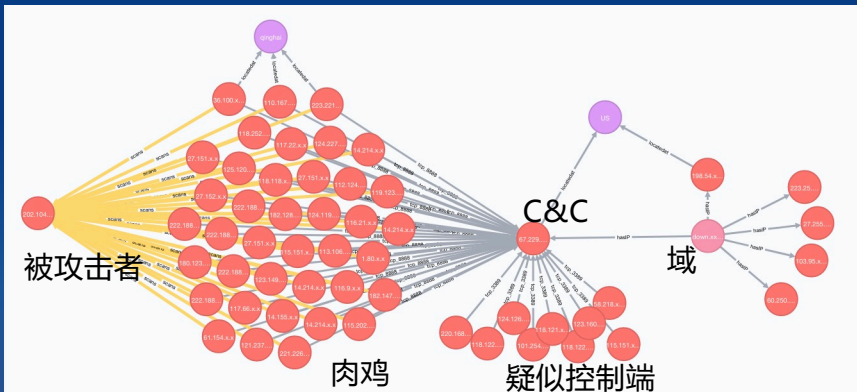
说得清 — 数据分析的能力

- Netflow与拓扑结合的攻击源定位
 - 还记得那个ingress index吗
- BOT交互特征与全网DPI分析
- 控制端 (C2) 的域名族分析

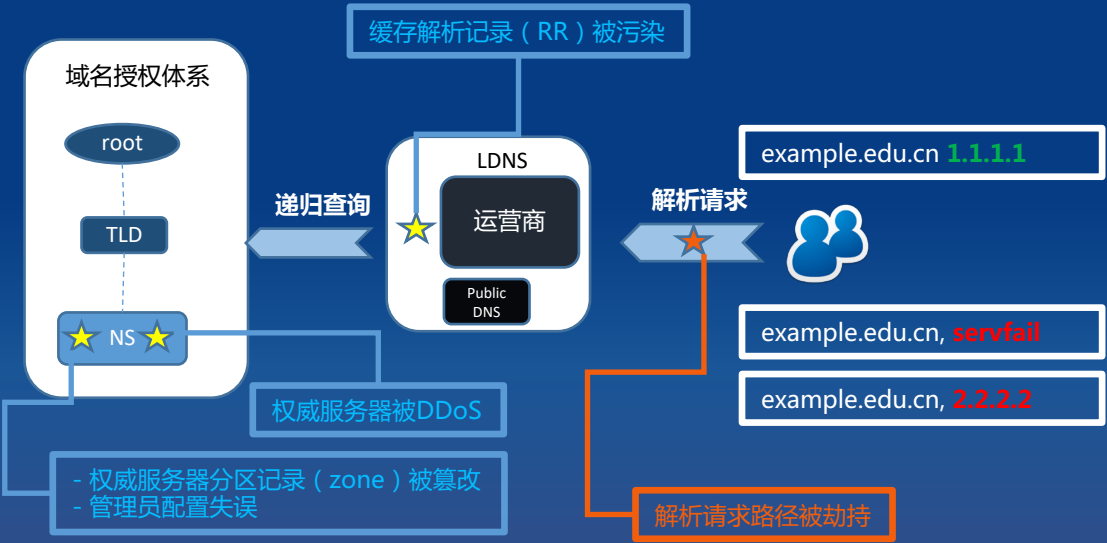
基于域名数据
分析僵尸网络Necurs C2
(word2vec)



Domain; IP Address; Port; Proto; Geo Info;



DNS安全



案例参考

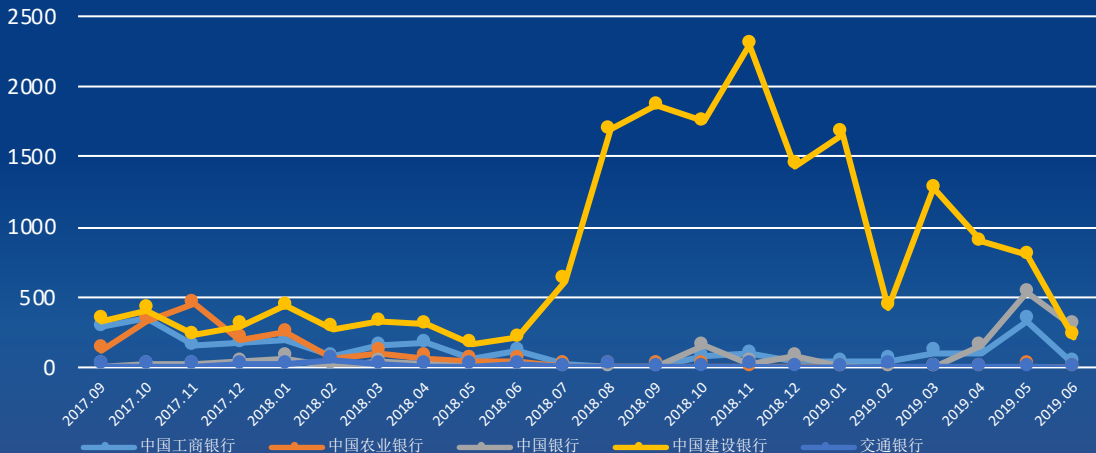
- “Lessons Learned from May 19 China’ s DNS Collapse” --DNS-OARC Workshop Nov 2009
- “DNS安全的这些年，那些事...” 中国计算机网络安全大会，2014年5月
- “智能设备，DDoS攻击的蓝海” 中国计算机网络安全大会，2015年5月
- “以全网之力，抗攻击之害” CSA，2016年10月
- “飞跃迷雾，把攻击看清楚” CCF YOCEF，2016年11月



DNS是互联网的黄页
它天然能够输出看见的能力和控

仿冒欺诈

针对五大行的仿冒站点 (数据来源: 云堤2017年9月~2019年06月23号)



仿冒网站监测案例

2017年5月31日 通过分析新增DNS域名解析发现三例仿冒湖北银行的钓鱼网站 www.hubeibank.cn.b0lw.cn ;
www.hubeibank.cn.evsgc.cn ; www-hubeibank-cn.zqv6f.cn, 并且根据其中一个钓鱼网站的IP 107.165.81.57 从Passive DNS和DPI数据关联分析挖掘查出针对我国62个商业银行/证券的钓鱼网站！

长白山水农村商业银行	www.cbmnsh.com.b0lw.cn
浙江宁波银行	www.nbc.cn.b0lw.cn
浙江稠州商业银行	www.czcb.com.cn.b0lw.cn
长春发展农商银行	www.cdcb.com.b0lw.cn
云南红塔银行	www.yxcb.com.cn.b0lw.cn
营口沿海银行	www.coastalbank.cn.b0lw.cn
新疆乌鲁木齐银行	www.uccb.com.cn.b0lw.cn
湘潭农商银行	www.xtrcb.net.b0lw.cn
四川绵阳市商业银行	www.mysyhh.com.b0lw.cn
四川泸州市商业银行	www.lzccb.cn.b0lw.cn
四川达州市商业银行	www.dzccb.com.cn.b0lw.cn
衡水农商银行	www.sxsmrcb.com.b0lw.cn
上海浦发硅谷银行	www.spd-svbank.com.b0lw.cn
陕西长安银行	www.ccabcchina.com.b0lw.cn
陕西杨凌农村商业银行	www.yrcbank.net.b0lw.cn
陕西绥德农商银行	www.sxsdsnyh.com.b0lw.cn
陕西米脂农商银行	www.mznsyh.com.b0lw.cn
山西长治潞州农村商业银行	www.czrcb.net.b0lw.cn
山西长治黎都农村商业银行	www.lidubank.com.b0lw.cn
山东烟台银行	www.yantaibank.net.b0lw.cn
山东威海市商业银行	www.whccb.com.b0lw.cn

三门峡湖滨农村商业银行	www.smxhbrcb.com.b0lw.cn
宁波农商银行	www.ncrcb.net.b0lw.cn
宁波鄞县农村商业银行	www.cixibank.com.b0lw.cn
内蒙古五原农村商业银行	www.nmgwysnyh.com.b0lw.cn
南京银行	www.njcb.com.cn.b0lw.cn
名古屋银行	www.meigin.com.b0lw.cn
辽阳银行	www.bankofliaoyang.net.b0lw.cn
辽宁盛京银行	www.shengjingbank.com.cn.b0lw.cn
辽宁朝阳银行	www.cycb.com.b0lw.cn
开源证券	www.kysec.cn.b0lw.cn
江西上饶银行	www.srbank.cn.b0lw.cn
济宁银行	www.jn-bank.com.b0lw.cn
吉林福柯农村商业银行	www.jlyscb.com.b0lw.cn
吉林延边农商银行	www.ybnsyh.com.b0lw.cn
吉林省长春市双阳农商银行	www.synsyh.com.b0lw.cn
吉林蛟河农村商业银行	www.jljjhrcb.com.b0lw.cn
吉林环城农村商业银行	www.jlhrcb.cn.b0lw.cn
黄山太平农村商业银行	www.hstprcb.com.b0lw.cn
淮北农商银行	www.hbnsyh.com.b0lw.cn
华福证券	www.hfzq.com.cn.b0lw.cn
华宝证券	www.cnhbstock.com.b0lw.cn
湖南吉首农村商业银行	www.hnjsrcb.com.b0lw.cn

湖南华容农村商业银行	www.hrrcb.com.cn.b0lw.cn
湖南洞口农商银行	www.hndknsyh.cn.b0lw.cn
呼伦贝尔农村商业银行	www.hlbrcb.com.b0lw.cn
恒泰长财证券有限责任公司	www.ccqzq.net.b0lw.cn
河南伊川农村商业银行	www.yichuanrcb.cn.b0lw.cn
河南新郑农村商业银行	www.xznsyh.com.b0lw.cn
河南焦作中铝银行	www.jzctb.com.b0lw.cn
河南汴京农村商业银行	www.hnbjbank.com.b0lw.cn
河北衡水银行	www.hengshuibank.com.b0lw.cn
广西资源农村商业银行股份有限公司	www.zyncsyhh.com.b0lw.cn
广东中山农村商业银行	www.zsebank.com.b0lw.cn
广东揭阳农村商业银行	www.jyebank.com.b0lw.cn
福建石狮农商银行	www.ssrcb.com.b0lw.cn
东方财富证券	www.xzsec.com.b0lw.cn
大连农商银行	www.dlrcb.cn.b0lw.cn
包头农商银行	www.baorcb.com.b0lw.cn
安徽宣城皖南农村商业银行	www.xcwncrb.com.b0lw.cn
安徽芜湖沱牌盛农村商业银行	www.whjsrcb.com.b0lw.cn
安徽淮南通商银行	www.hcrcb.com.b0lw.cn

数据资源和访问路径的控制力的挖潜开放
使得仿冒欺诈的发现和处置能力明显升级

路由安全

对路由的理解将决定对大网安全的理解
也将直接决定业务承载的安全

还记得825的案例吗

案例

Possible BGP hijack

Beginning at 2018-09-18 12:50:33, we detected a possible BGP hijack.

Prefix 203.107.32.0/22, Normally announced by AS37963 Hangzhou Alibaba Advertising Co.,Ltd.


Starting at 2018-09-18 12:50:33, a more specific route (203.107.32.0/24) was announced by ASN 8100.

This was detected by 192 BGPMon peers.

Expected

Start time: 2018-09-18 12:50:33 UTC

Expected prefix: 203.107.32.0/22

Expected ASN: 37963  (Hangzhou Alibaba Advertising Co.,Ltd.)

Event Details

Detected advertisement: 203.107.32.0/24

Detected Origin ASN 8100  (QuadraNet, Inc)

Detected AS Path 49362 3356 6461 22298 8100

Detected by number of BGPMon peers: 192

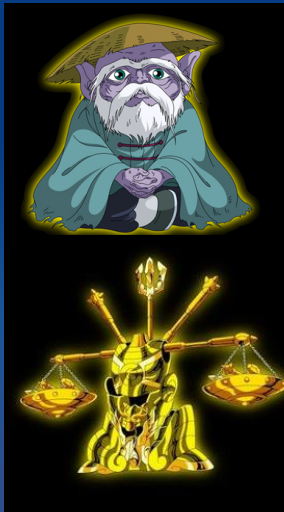
云堤具有完整的互联网侧防护能力



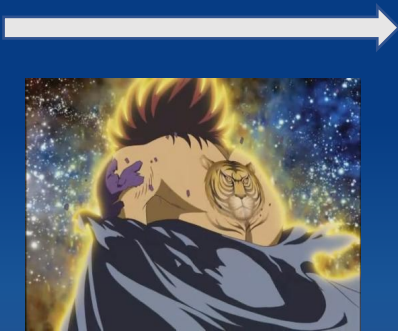
稀缺性 – 绝对意义上的少有，少见
差异化 – 相对意义上的人无我有，人有我强

功能的稀缺保证产品能力差异化
运营的高效保证客户体验差异化

觉醒



转变



发力

