



借网络之力，护网络安全

刘紫千

中国电信

GITC2016，北京



互联网+环境下，主要的网络安全威胁来自 ...

- DDoS攻击
- 域名解析问题
- 欺诈钓鱼威胁
- Web安全威胁
- 其他（APT, 系统级漏洞, 业务逻辑问题 ...）

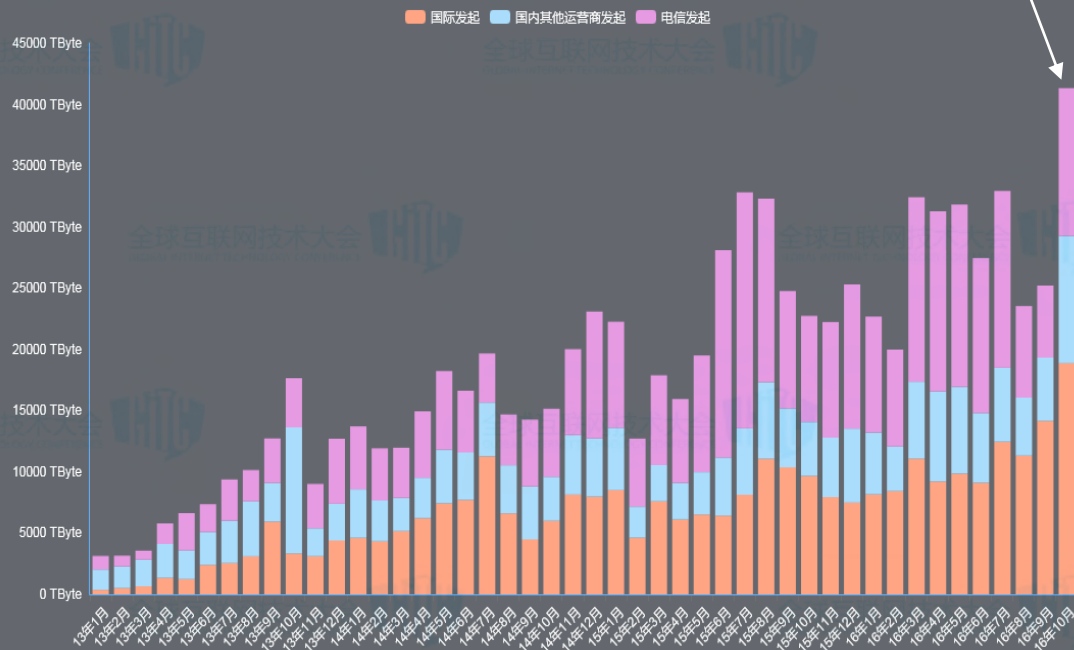
主要网络安全威胁 – DDoS攻击 (来自: 云堤抗D damddos.com)

峰值
41328TByte
2016年10月

某客户遭受DDoS攻击

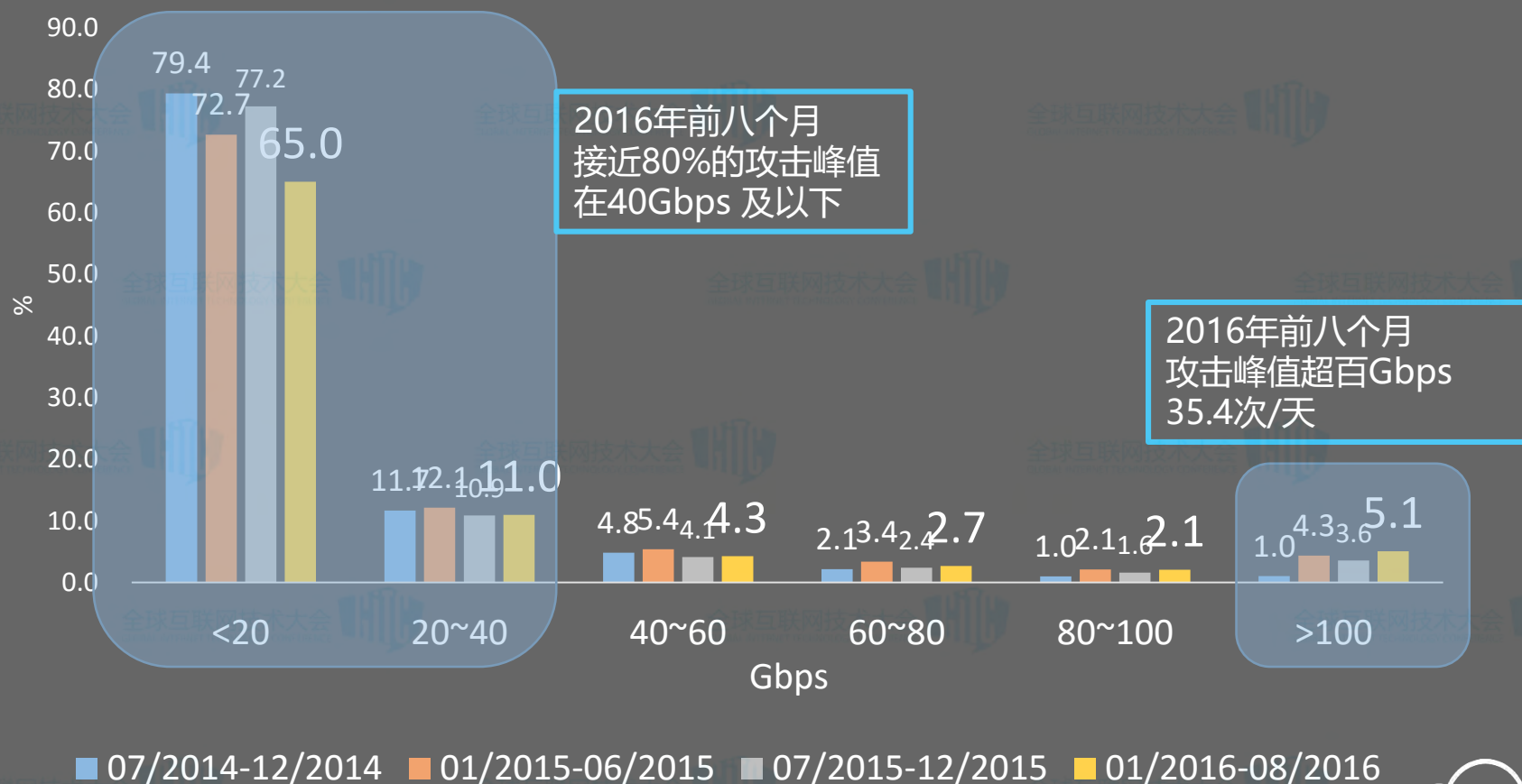


DDoS攻击趋势

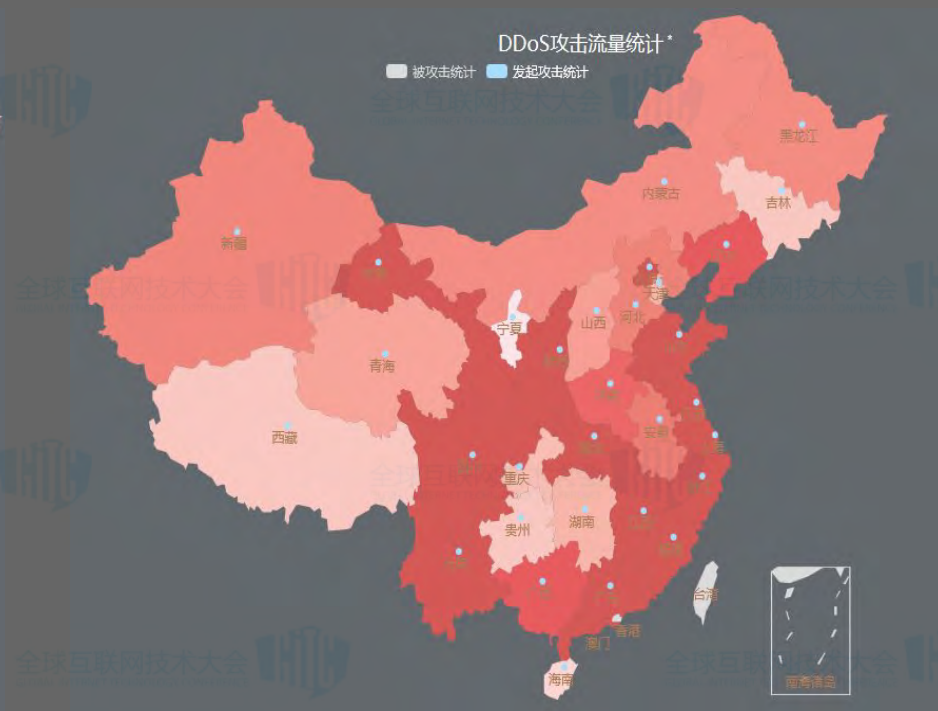
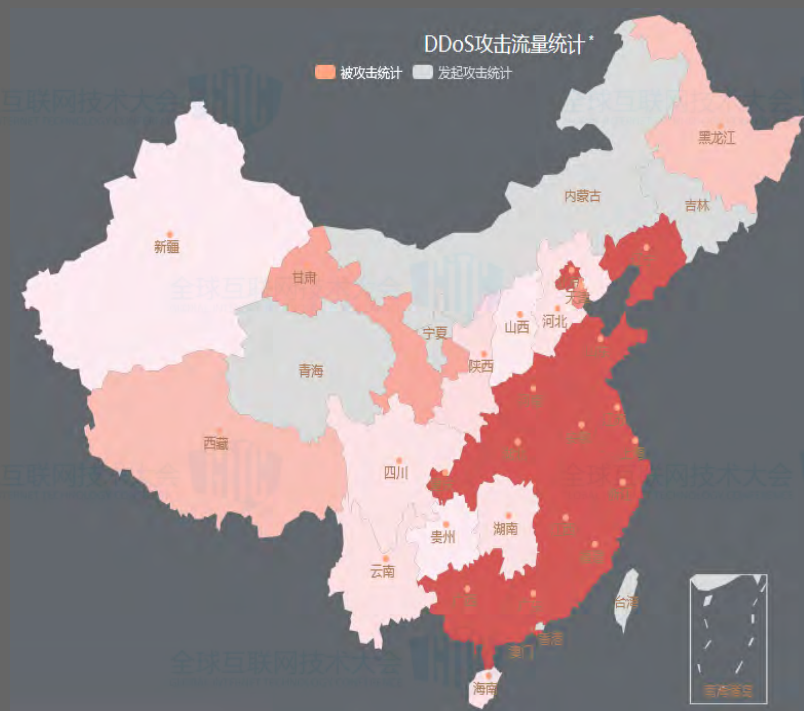


如此规模的攻击，单靠客户自身是无法抵抗的

连续四个半年DDoS攻击峰值分布对比



被攻击地域多为经济发达地区，但发起攻击地域则不然



攻击载体 & 攻击方式

- 载体：PC → IDC/物理服务器/网络设备 → 云（VPC）→ IoT
- 向量：简单 → 复杂 → 简单
- 攻击发起源：真实源IP（UDP反射、CC）+ 虚假源IP（境外流量）
- 攻击控制源：境外的多级跳板

攻击的动机

- 商业竞争
- 政治主张
- 敲诈勒索
- 意见相左
-

云堤-抗D的演进

- 关于清洗

- 新增北美、欧洲、亚太三个方向10个近源清洗点，骨干防护节点总数扩展至36个
- 全球清洗容量突破2T
- 新增云堤高防节点，为客户提供容量更有弹性、成本更低、双线的清洗服务

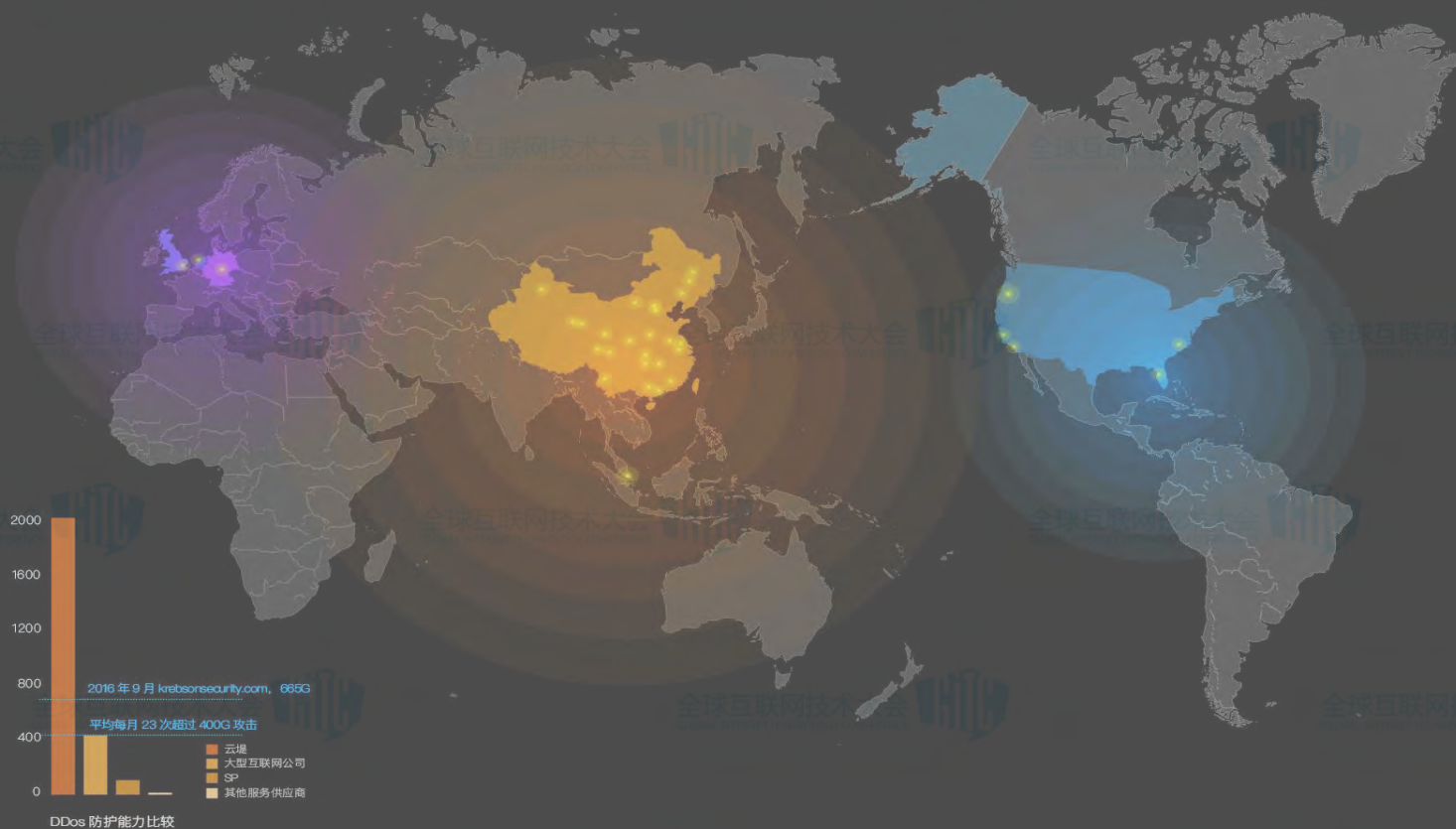
- 关于压制

- 近源覆盖国内重点省IDC出向流量
- 对原有国际方向流量细分到大洲和部分国家

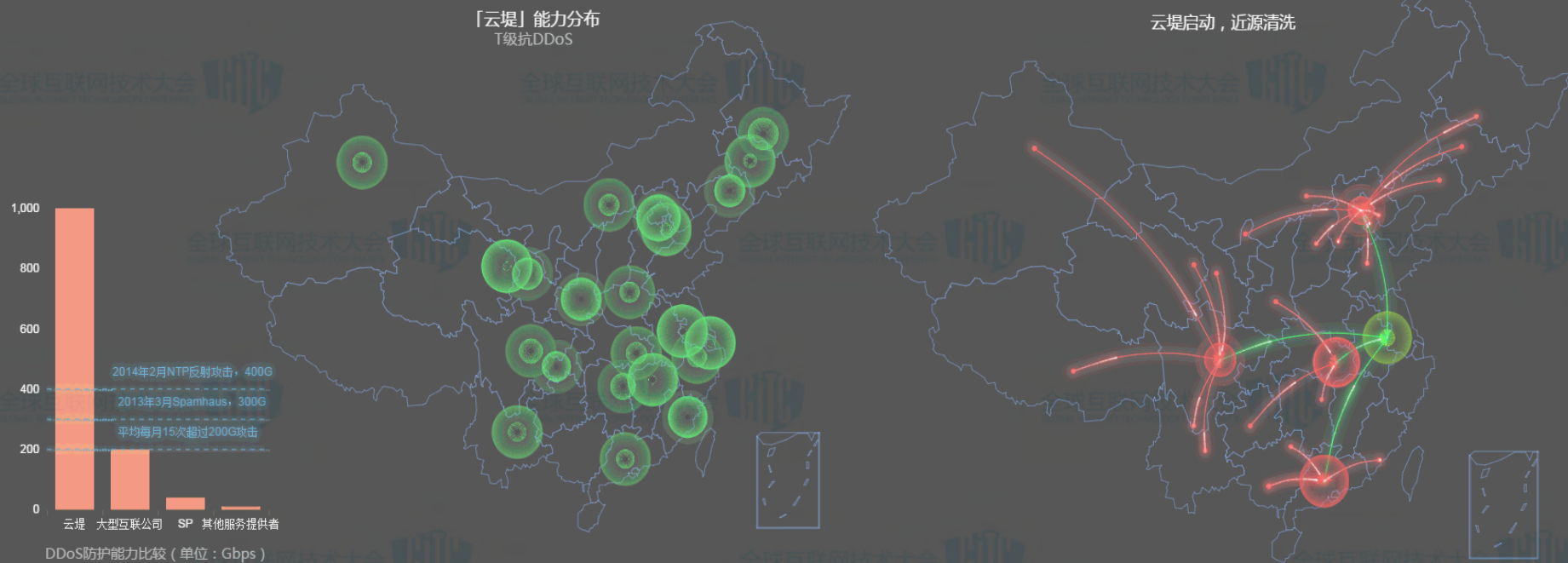
- 联合倡议发起“云清联盟”



云堤抗D-清洗防护节点全球分布



近源防护 — 分布部署、集中调度、分而治之、化整为零



客户如何使用云堤-抗D？

- 400专家热线
- 自服务Portal
- 微信客户端
- API



不得不说的一次“DDoS攻击”...

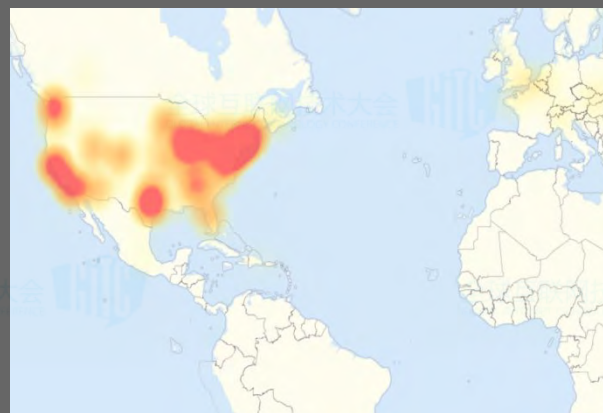
• DYN

• DDoS Event

Update Regarding DDoS Event
Against Dyn Managed DNS on
October 21, 2016
Incident Report for Dyn, Inc.

• 大面积业务瘫痪！

• Airbnb ^[12]	• Etsy ^{[12][16]}	• Netflix ^{[14][20]}	• Second Life ^[27]	• Verizon Communications ^[17]
• Amazon.com ^[9]	• FiveThirtyEight ^[14]	• The New York Times ^{[12][17]}	• Shopify ^[12]	• Visa ^[28]
• Ancestry.com ^{[13][14]}	• Fox News ^[20]	• Overstock.com ^[14]	• Slack ^[24]	• Vox Media ^[30]
• The A.V. Club ^[15]	• The Guardian ^[20]	• PayPal ^[16]	• SoundCloud ^{[12][19]}	• Walgreens ^[14]
• BBC ^[14]	• GitHub ^{[12][17]}	• Pinterest ^{[17][19]}	• Squarespace ^[14]	• The Wall Street Journal ^[20]
• The Boston Globe ^[12]	• GrubHub ^[21]	• Pixlr ^[14]	• Spotify ^{[13][17][19]}	• Wikia ^[13]
• Box ^[16]	• HBO ^[14]	• PlayStation Network ^[17]	• Starbucks ^{[13][23]}	• Wired ^[16]
• Business Insider ^[14]	• Heroku ^[22]	• Qualtrics ^[13]	• Storiify ^[16]	• Wix.com ^[31]
• CNN ^[14]	• HostGator ^[14]	• Quora ^[14]	• Swedish Civil Contingencies Agency ^[28]	• WWE Network ^[32]
• Comcast ^[17]	• iHeartRadio ^{[13][23]}	• Reddit ^{[13][17][19]}	• Swedish Government ^[28]	• Xbox Live ^[33]
• CrunchBase ^[14]	• Imgur ^[24]	• Roblox ^[26]	• Tumblr ^{[13][17]}	• Yammer ^[24]
• DirecTV ^[14]	• Indiegogo ^[13]	• Ruby Lane ^[14]	• Twilio ^{[13][14]}	• Yelp ^[14]
• The Elder Scrolls Online ^{[14][18]}	• Mashable ^[26]	• RuneScape ^[13]	• Twitter ^{[12][13][17][19]}	• Zillow ^[14]
• Electronic Arts ^[17]	• National Hockey League ^[14]	• SaneBox ^[22]		
		• Seamless ^[24]		



云堤看见 ... Part1

- DYN把客户NS分布在四个/24网段
 - 208.78.70.A ns1.pA.dynect.net
 - 204.13.250.B ns2.pB.dynect.net
 - 208.78.71.C ns3.pC.dynect.net
 - 204.13.251.D ns4.pD.dynect.net

- Pfx → ASN : AS33517

- 全网AS path

- 到208.78.70.0/24和208.78.71.0/24的路径 : 2914 33517
- 到204.13.250.0/24和204.13.251.0/24路径 : 1299 33517

- 电信骨干网与AS1299 (Telia) 和AS2914 (NTT) 的互联电路流量是否有突发

- 10月21日20:00 - 22:20
- 10月22日00:52
- 10月22日05:00 - 07:11
(UTC + 8)

;; ANSWER SECTION:

box.com.	83133	IN	NS	ns-1314.awsdns-36.org.
box.com.	83133	IN	NS	ns-200.awsdns-25.com.
box.com.	83133	IN	NS	ns-1820.awsdns-35.co.uk.
box.com.	83133	IN	NS	ns4.p05.dynect.net.
box.com.	83133	IN	NS	ns-891.awsdns-47.net.
box.com.	83133	IN	NS	ns2.p05.dynect.net.
box.com.	83133	IN	NS	ns1.p05.dynect.net.
box.com.	83133	IN	NS	ns3.p05.dynect.net.

;; ANSWER SECTION:

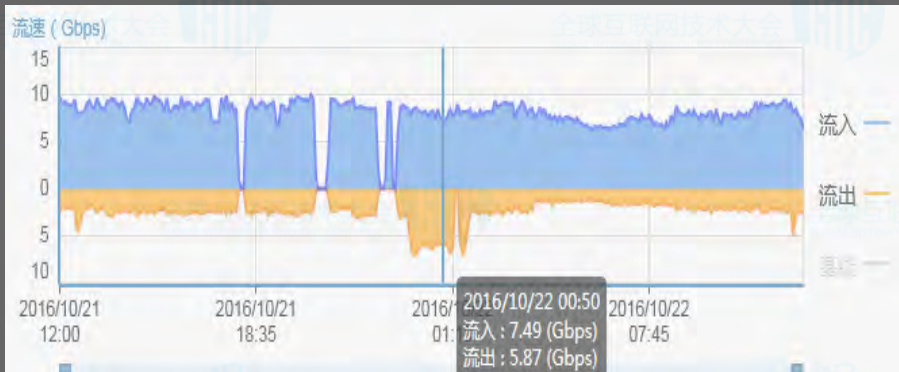
twitter.com.	6932	IN	NS	ns3.p34.dynect.net.
twitter.com.	6932	IN	NS	ns2.p34.dynect.net.
twitter.com.	6932	IN	NS	ns4.p34.dynect.net.
twitter.com.	6932	IN	NS	ns1.p34.dynect.net.

;; ANSWER SECTION:

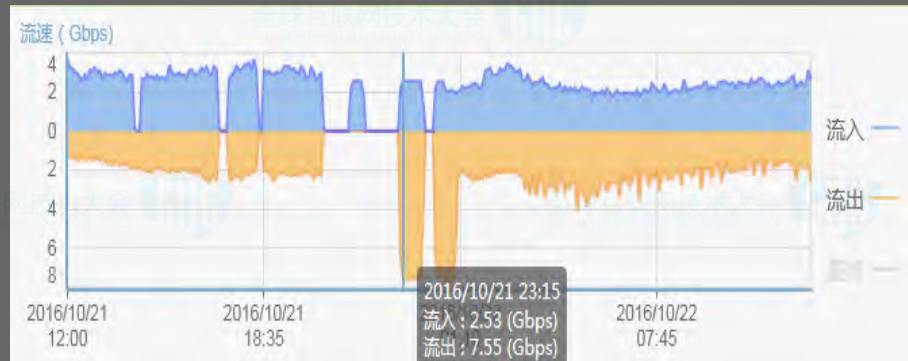
paypal.com.	300	IN	NS	ns2.p57.dynect.net.
paypal.com.	300	IN	NS	pdns100.ultradns.net.
paypal.com.	300	IN	NS	ns1.p57.dynect.net.
paypal.com.	300	IN	NS	pdns100.ultradns.com.



AS2914 Telia

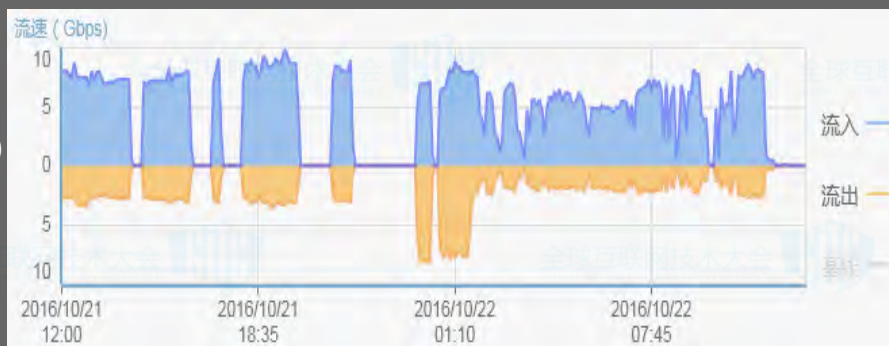
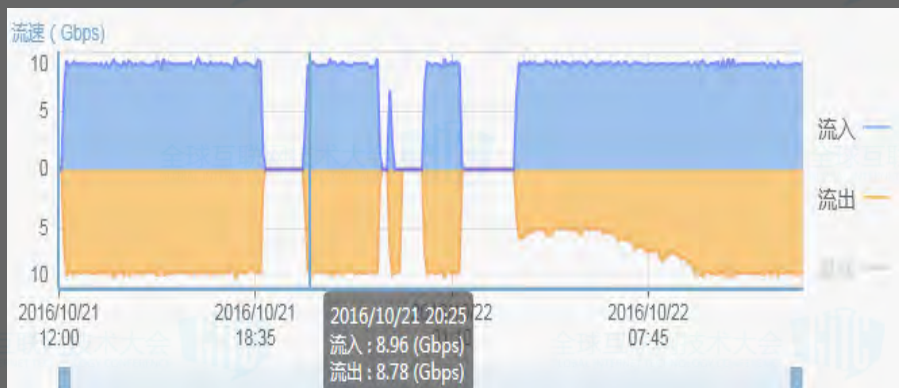


AS1299 NTT -LDN

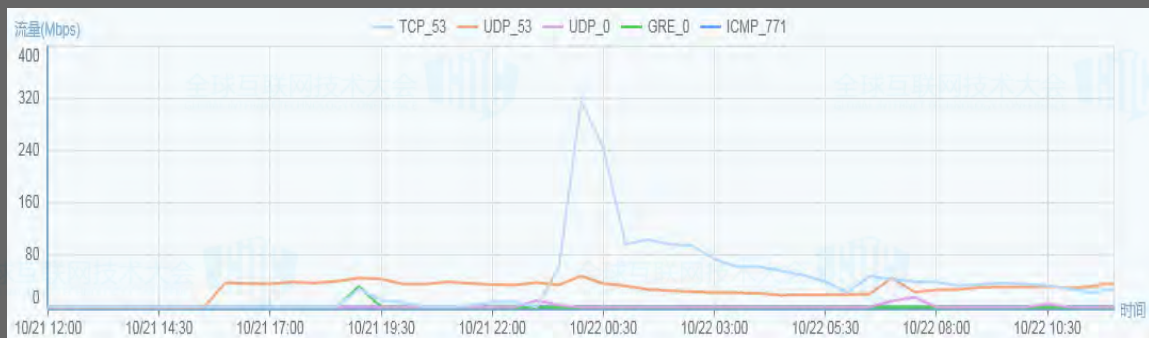
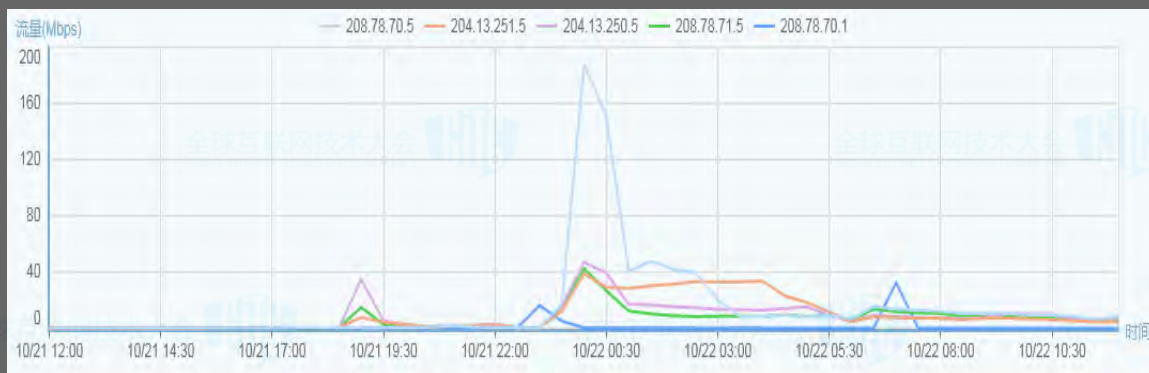
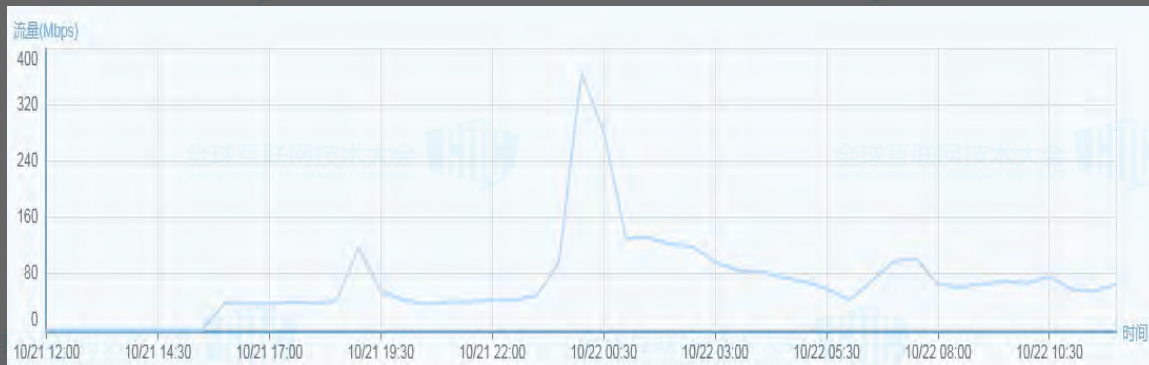


云堤看见 ... Part2

- 累计流量突增 < 40Gbps
- 这只是peer直连电路汇总流量
- 需要进一步检查去往AS33517特定网段的Netflow流量



DYN的4个C段地址的流量成分分析



云堤看见 ... Part3

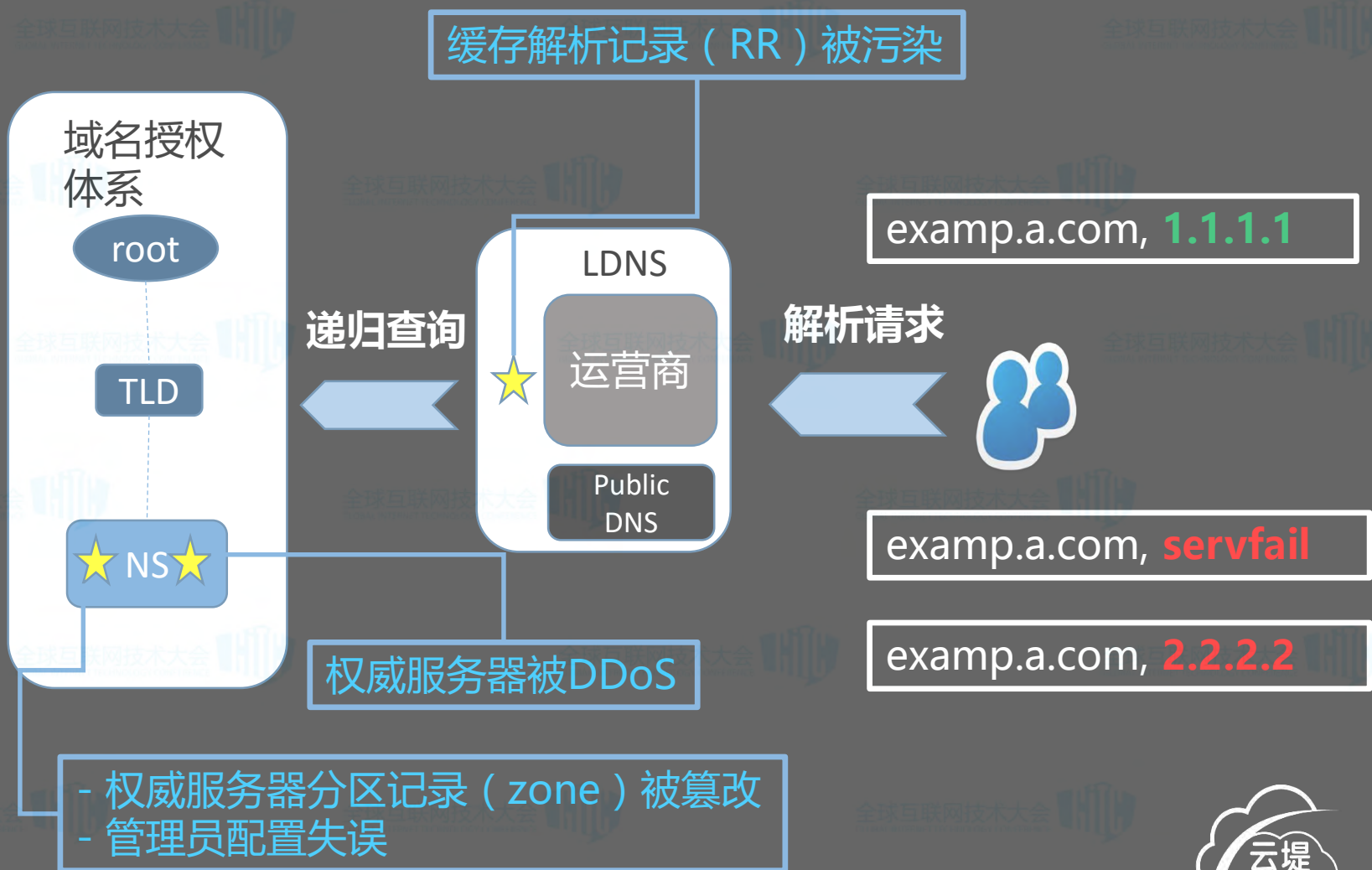
- 中国电信全网流向4个C段地址的流量累积峰值 <400Mbps
- ns[1-4].p05.dynect.net 这组服务器流量最大
- TCP53、UDP53流量居多
- 曾记否，519...

互联网+环境下，客户面临的主要网络安全威胁

- DDoS攻击
- 域名解析问题
- 欺诈钓鱼威胁
- Web安全威胁



DNS域名解析会遇到什么安全问题？



客户DNS域名安全防护的...

理想：

- 高效监控全网解析异常
- 域名解析不对了，赶快恢复！
- 授权服务不会瘫痪

疑问：秒级？全网？不可能吧...

现实：我们做到了！

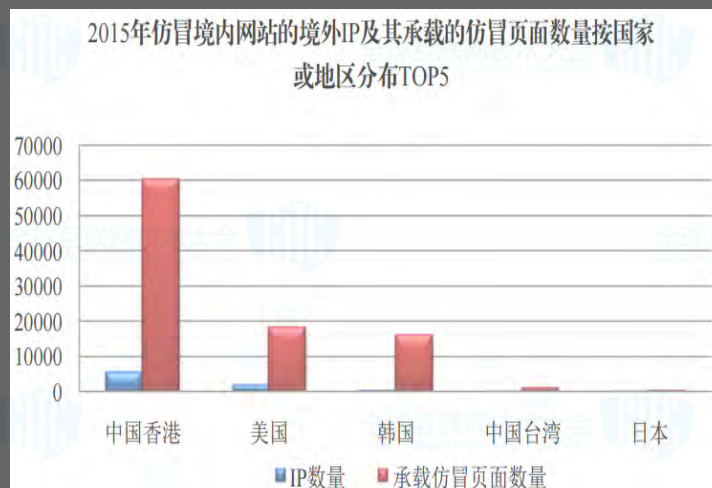
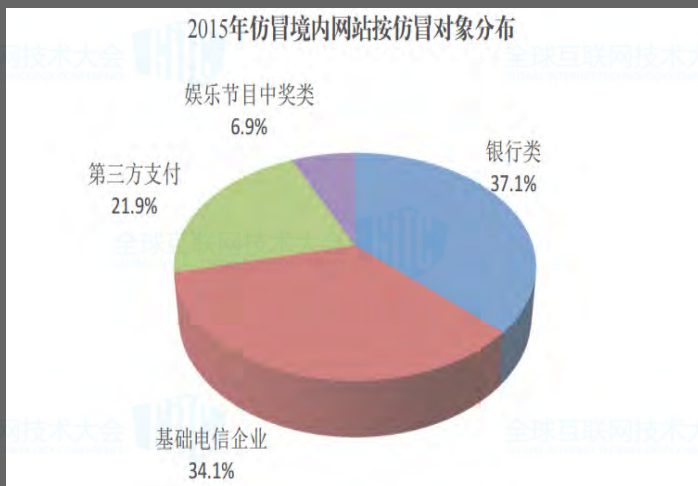


互联网化环境下，金融行业面临的主要网络安全威胁

- DDoS攻击
- 域名解析问题
- 欺诈钓鱼威胁
- Web安全威胁

钓鱼网站已经非常猖獗了...

- **手段**：电话诈骗、邮件欺诈、短信欺诈、恶意APP、二维码恶意链接、WiFi等
- **影响**：网络钓鱼每年全国影响人次过亿，造成数百亿金额损失，损失金额近5年年复合增长率超32.3%
- **趋势**：CNCERT 监测数据发现
 - 2015 年针对我国境内网站的仿冒页面数量较 2014 年增长 85.7%。其中，针对金融支付的仿冒页面数量上升最快，较 2014 年增长 6.37 倍；在针对我国境内网站的仿冒站点中，83.2%位于境外
 - 2016 年 1-6月，在针对我国境内网站的仿冒站点中，75%以上都境外，主要位于中国香港和美国

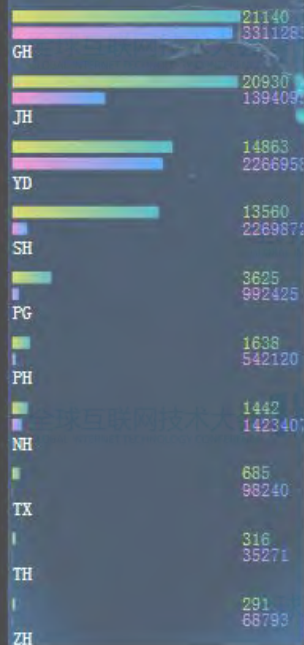


钓鱼网站统计
(自2016-01-01累计)

钓鱼网站发现数 **97,323** 受骗访问钓鱼网站次数 **88,530,033**
估测用户受骗金额 **9,307,638,722** 元

钓鱼网站仿冒对象TOP10

■ 钓鱼网站数 ■ 网站访问次数



2016-11-11 13:30:37	中国	118.193.242.21	http://wap.ccbawy.cc	建设银行
2016-11-11 13:30:37	美国	23.252.166.28	http://95588.pipq-1.pw	工商银行
2016-11-11 13:30:37	中国	150.129.80.53	http://wap.ccbbsm.cc	建设银行
2016-11-11 13:30:37	中国	123.1.152.135	http://wap.ccbuet.cc	建设银行
2016-11-11 13:30:37	中国	123.1.152.135	http://wap.ccbuet.cc	建设银行
2016-11-11 13:30:37	中国	118.193.242.21	http://wap.ccbawy.cc	建设银行
2016-11-11 13:30:37	中国	45.120.185.48	http://wap.icdoc.cc	工商银行

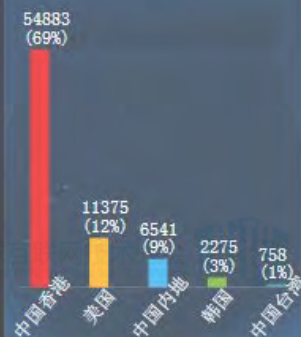
钓鱼网站域名



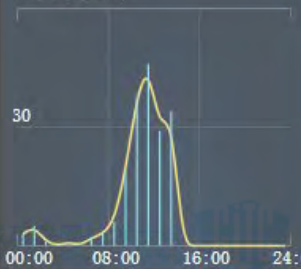
钓鱼网站访问方式



钓鱼网站所在地TOP5

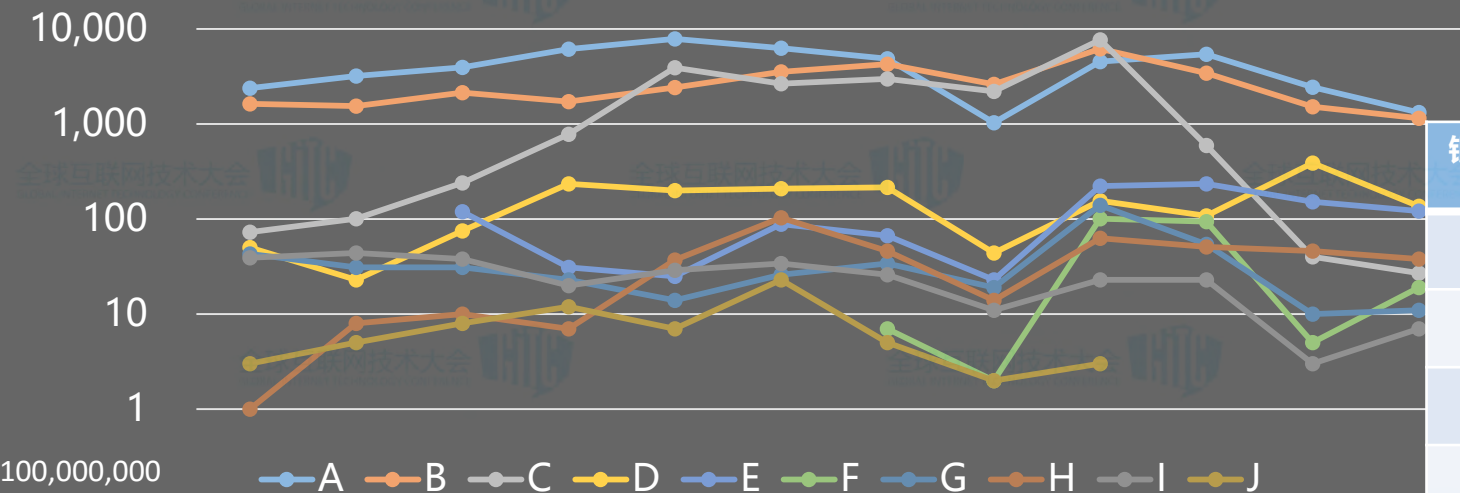


今日钓鱼态势



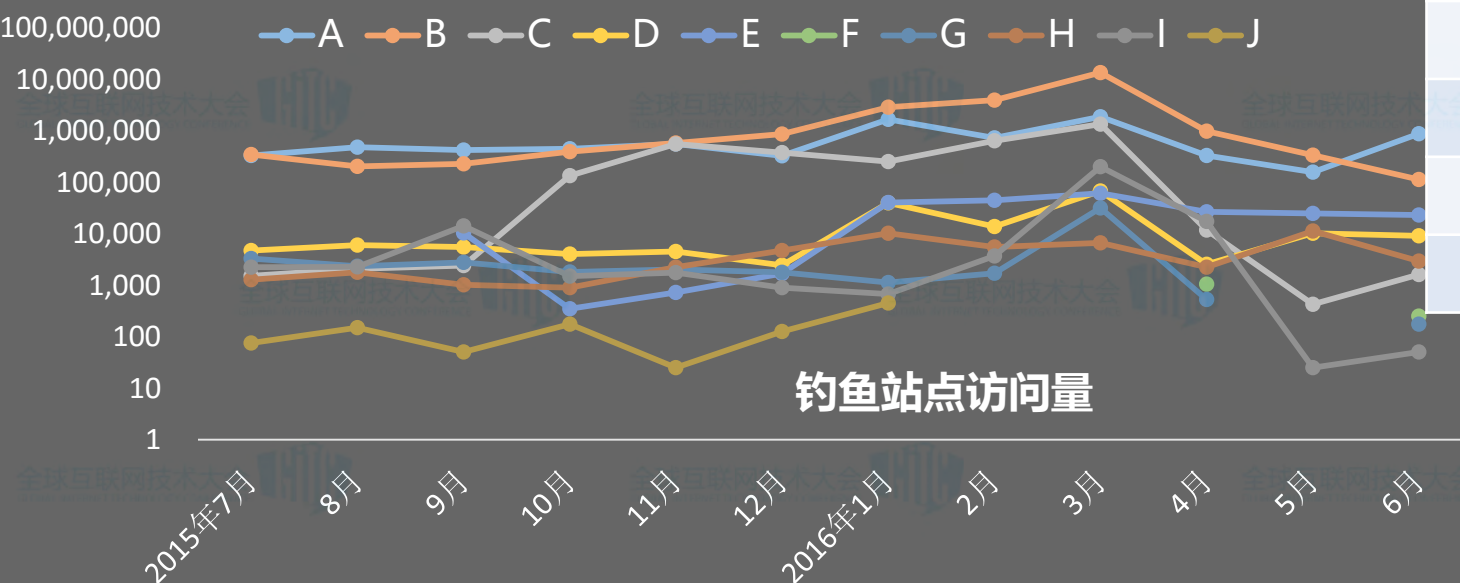
「云堤-反钓鱼」的监测数据

钓鱼仿冒站点数量



银行	钓鱼网站数量(url/月)	访问次数(次/月)
A	4,108	683,631
B	2,673	2,040,613
C	1,769	277,931
D	153	14,210
E	108	23,420
...
I	25	20,548

钓鱼站点访问量



钓鱼网站的应对必须满足

- 及时准确的发现最新钓鱼网站
- 迅速阻断钓鱼站点的访问
- 移动环境的普适性，不用插件（与终端类型不相关，比如iphone）
- 深度数据挖掘，精准的风控

互联网化环境下，金融行业面临的主要网络安全威胁

- DDoS攻击

- 域名解析问题

- 钓鱼网站威胁

- Web安全威胁



Web安全威胁

关注点

- OWASP TOP10
- 业务逻辑和资金交易安全

趋势

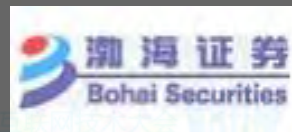
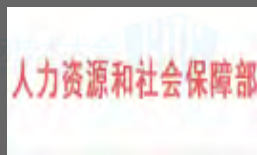
- 2015年全年
 - 我国境内被篡改网站数量为24550个, 被植入暗链的网站占全部被篡改网站的比例高达83% ;
 - 共监测到境内75028个网站被植入后门
- 2016年上半年
 - 我国境内被篡改网站数量为36143个
 - 共监测到境内70503个网站被植入后门



对Web安全服务的要求

- 周期的自动化检测 + 人员投入
- 安全资讯和应急响应速度的比拼，高度动态
- 希望照顾全方位大覆盖范围（漏扫、WAF、防篡改、敏感字/错别字、访问稳定性），但真的没有百分之百的安全...

云堤已服务于...



云/DC --- 网 --- 端

纵深防御

合适的角色，擅长的事情

找到风险控制的最佳发力点





感谢聆听

更多了解的途径

- 官网 damddos.com
- 新浪微博、百度百科“电信云堤”

