

DDoS防护思路演进

NSFOCUS TechWorld 2015

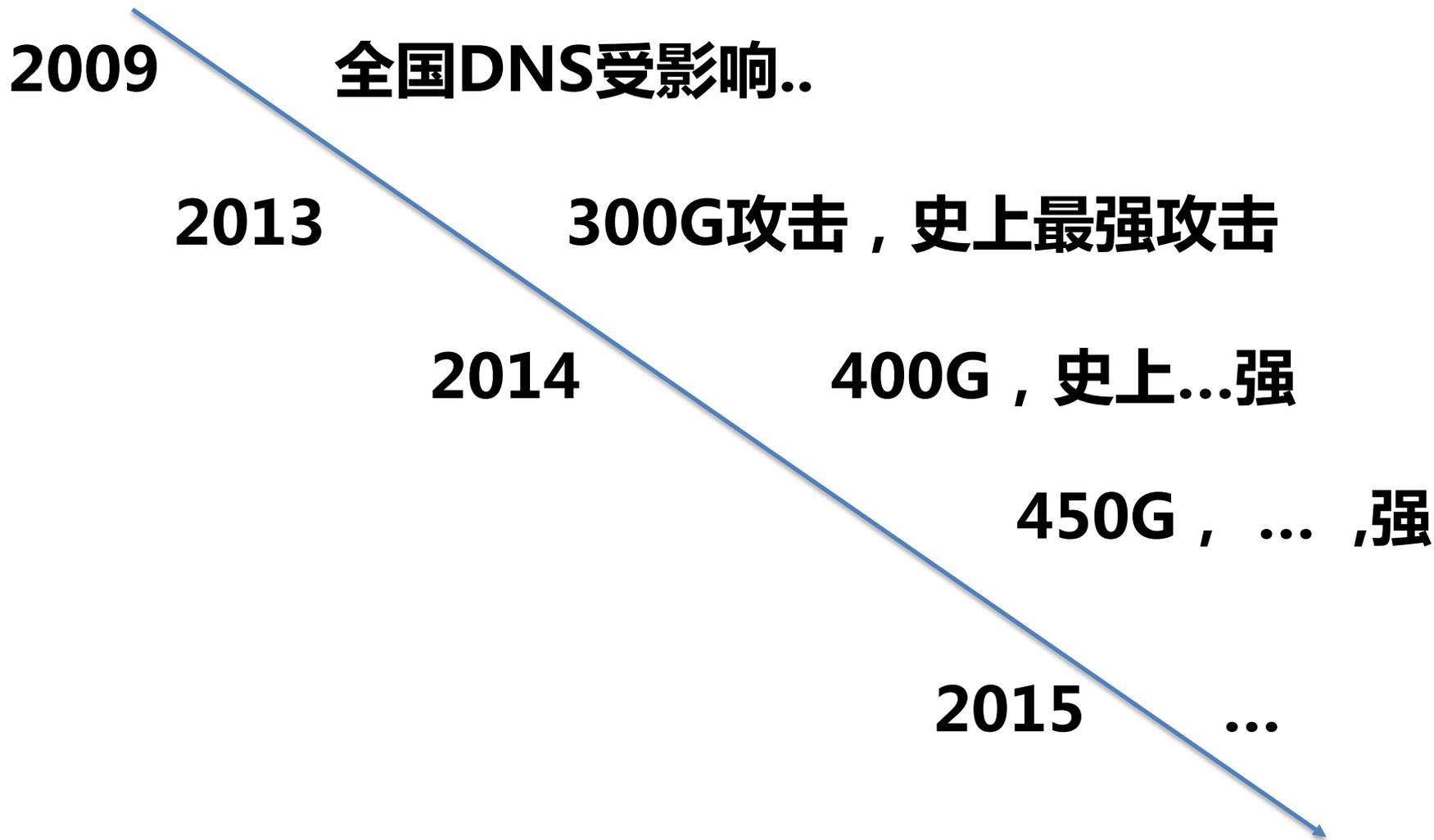
何坤

Because of the closed context of the original ARPANET and NSFNet, no consideration was given to denial-of-service attacks in the original Internet Architecture.

As a result, almost all Internet services are vulnerable to denial-of-service attacks of sufficient scale

——RFC4732

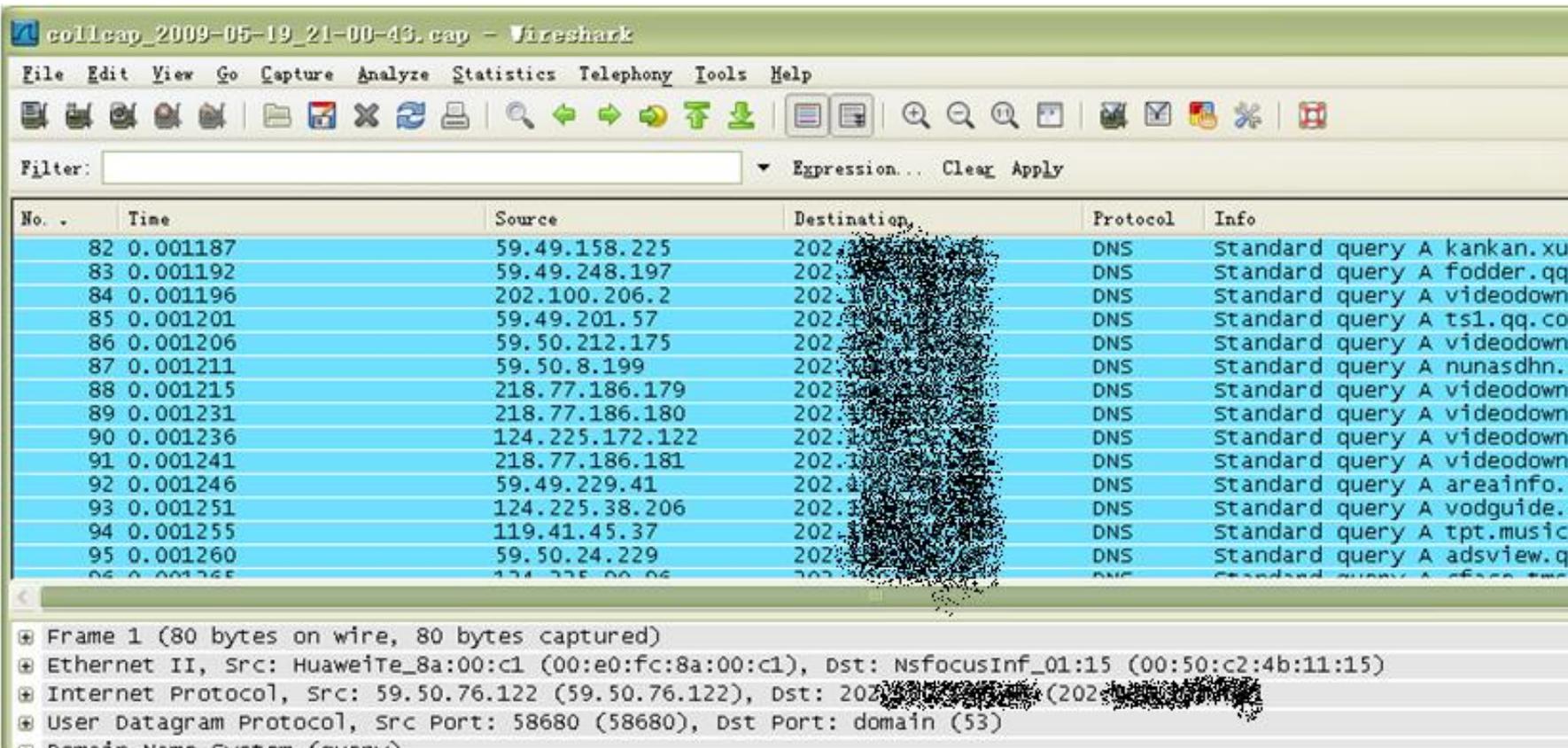
从一些事件说起



- 那些年的攻击，10G以下为主
 - 黑洞ADS4000系列
- SYN-FLOOD攻击
 - 独领风骚，常青树
 - 变种（SYN+ECN标志位等）
- HTTP-GET-FLOOD（CC）
 - 挑战黑洞—Challenge Collapsar
 - 见腾讯出的一篇文章
 - 《CC攻击，因误会而产生的十年网络安全浩劫》

- **DDoS开始严重影响互联网基础设施**
- **各地DNS开始实行区域访问**
 - **即本省的IP地址才可以访问**
 - **GEOIP防御思路的一种形式**

5.19 异常流量样本



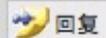
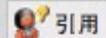
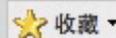
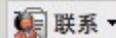
基于域名的学习、过滤
业务的正常模型

- **300G的DNS反射攻击**
- **US-CERT发布预警，并提供建议**
 - **DNS限定区域访问，同时进行源压制**
 - **类似5.19后国内运营商的方案**
- **DDoS这种攻击方式成为全球焦点**
- **反射、放大的攻击手法开始被争相使用，轻松上百G**
- **业界开始关注Cloudflare的大流量清洗技术**

400G , 2014年

3年前 , 内网论坛...

回复: ntp的安全问题

 回复  引用  收藏  联系

跟踪了一下这个问题, Internet上允许monlist的ntpd还不少, 我们的内网就N多, 大大超过我的想像。

让我们设想一下, 写脚本实现, 读取NTP Server List, 向这些NTP Server发送listpeers命令, 以此获取更多的NTP Server, 这个过程类似扫描Skype的超级结点。向所有的NTP Server发送monlist命令, 伪造monlist命令的源IP, 于是所有monlist响应会发往victim。monlist的请求与响应报文个数比是1:N, N一般都是几十甚至过百, 放大效果很明显。这种DDoS, 从victim来看还不容易追查来源。

- **Unicast: One Machine, One IP**
 - 一个点的清洗容量是有限的
- **Anycast: Many Machines, One IP**
 - 路由就近原则，就近清洗
 - 多个清洗中心
- **国内实际上早就有了Anycast DDoS防御**

- 二级域名随机查询攻击
- 不是已经做了访问限制了吗？
- URPF策略的实施，虚假源也越来越少
- 然而，这并没有什么用

多省份 DNS 系统遭遇 DDoS 攻击

应急响应服务处理报告

■ 文档编号	NS [REDACTED]	■ 密级	商业机密
■ 版本编号	V1.0	■ 日期	[REDACTED]

- **攻击源来自省内，规避了GEOIP防御**
- **大量肉鸡源为网络摄像头、路由器**
- **这些设备大带宽+7*24小时在线很少升级**

2014 绿盟科技 DDoS 威胁报告
2014 DDoS THREAT REPORT

观点1：智能设备发起 DDoS 攻击数量明显增多

事件1：2014 年国内规模最大的 DDoS 攻击——1/3 攻击源是智能设备

观点2：沿海省市是受攻击的集中地区，广东依然是最严重的受害区域

观点3：18 点-23 点是 DDoS 开始攻击的主要时间段

观点4：UDP FLOOD 成为最主要的 DDoS 攻击方式

事件2：SSDP 反射式 DDoS 攻击实例分析

观点5：在线游戏已进入 DDoS 攻击目标前3

观点6：93% DDoS 攻击发生在半小时内



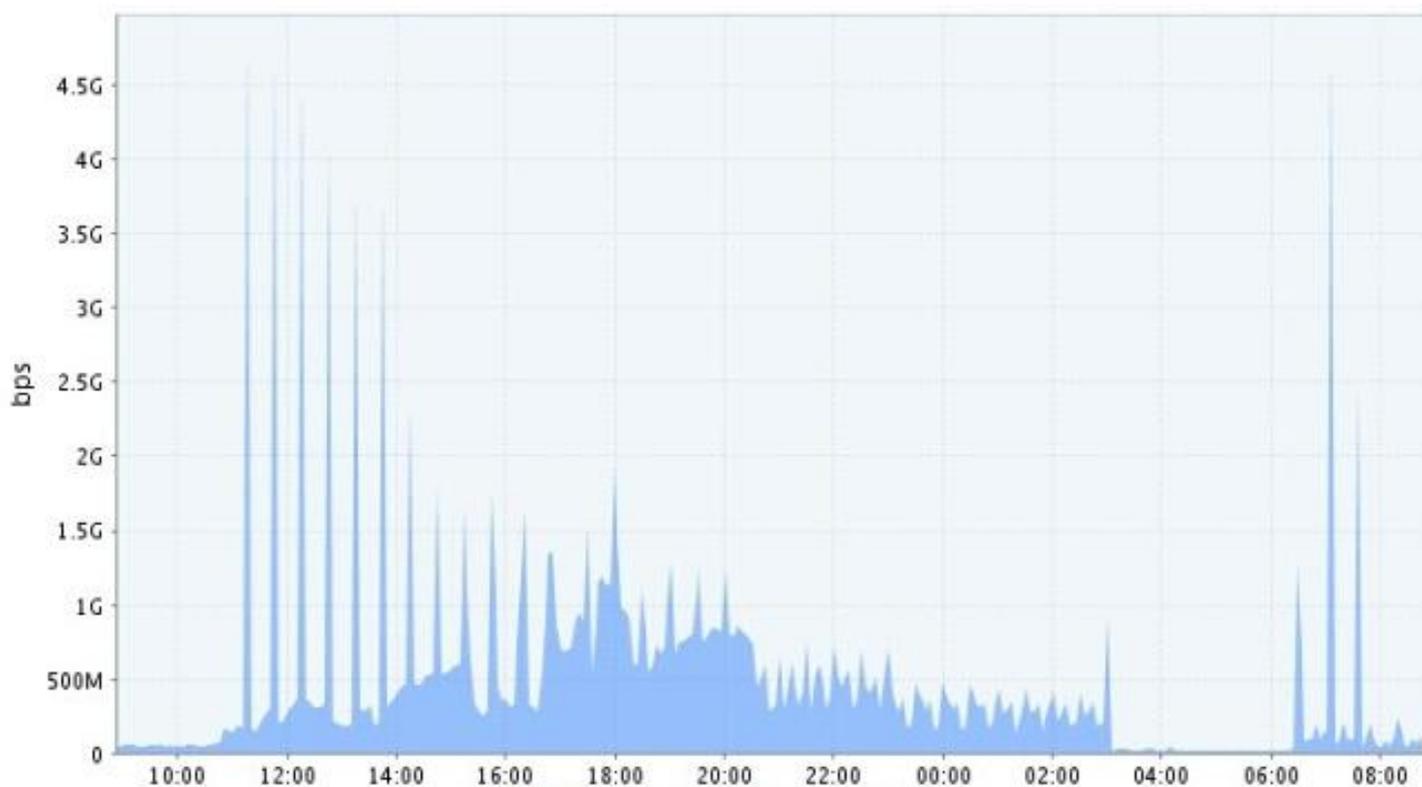
- 450G
 - SYN大包为主，而不是以反射为主，攻击者的资源很N
- 700G
- 以上都是小道消息，如有雷同，算我抄你的

如果是你，你会怎么攻？

- **百G+攻击**
 - 阵地战，拼资源
 - 掩人耳目
 - 资源的考验
- **应用层攻击**
 - 明修栈道，暗度成仓
 - 考验攻防经验、业务理解、运营能力
- **尽可能的以假乱真，让防御者无从下手**

脉冲式攻击

- 极短时间、多变的组合攻击，你可能连攻击类型都不知道
- 人工的防御手段难以应对
- 不怕贼偷，就怕贼惦记



SYN Flood

ACK Flood

DNS Flood

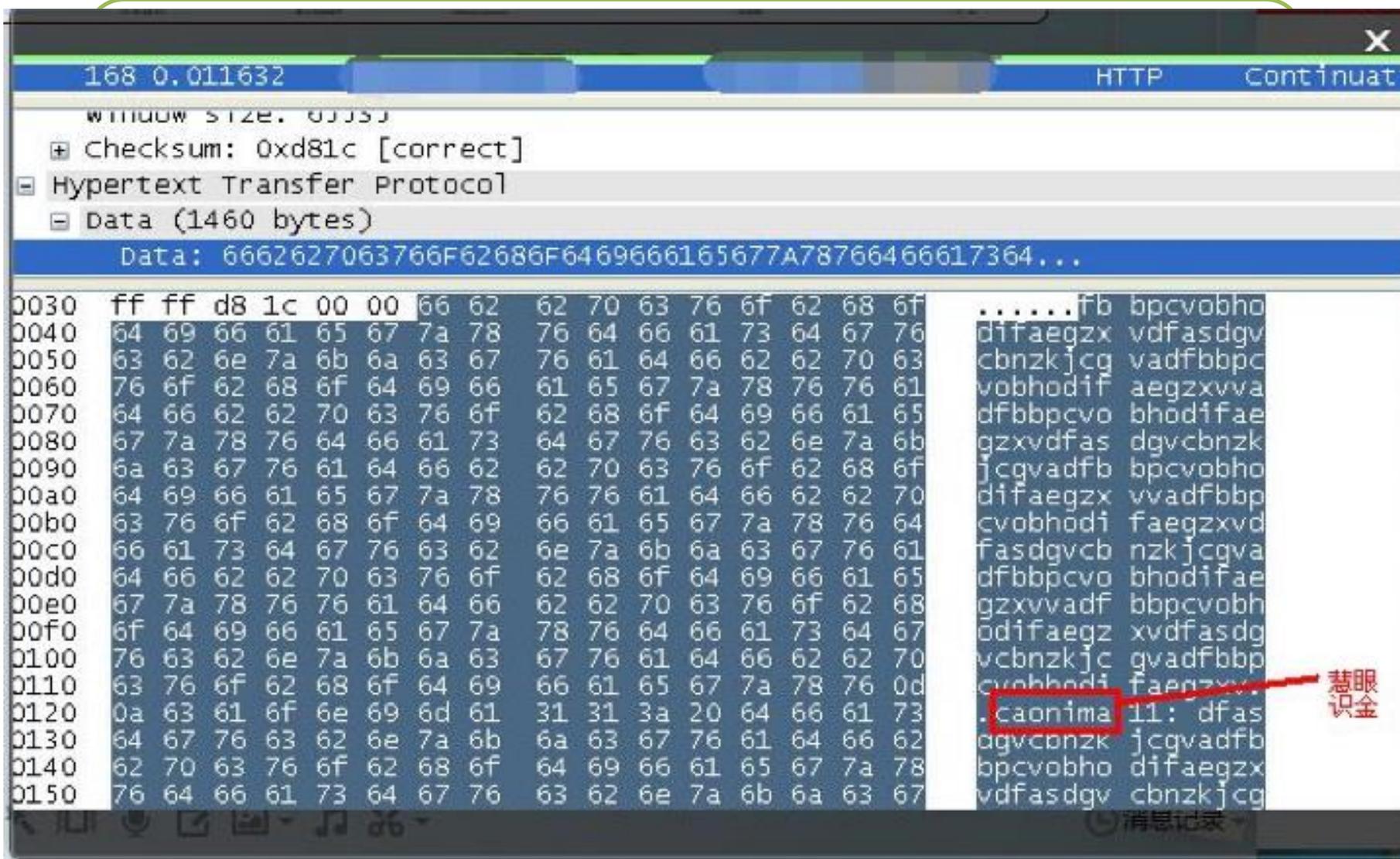
RESET Flood

等Spoofing Flood

反向探测/代理/Cookie

**思路：只要源IP能正确响应，则被认为是可信的
然而，真实源打出的攻击怎么应对？**

防御算法的演进



168 0.011632 HTTP Continuat

WINDOW SIZE: 0x3333

Checksum: 0xd81c [correct]

Hypertext Transfer Protocol

Data (1460 bytes)

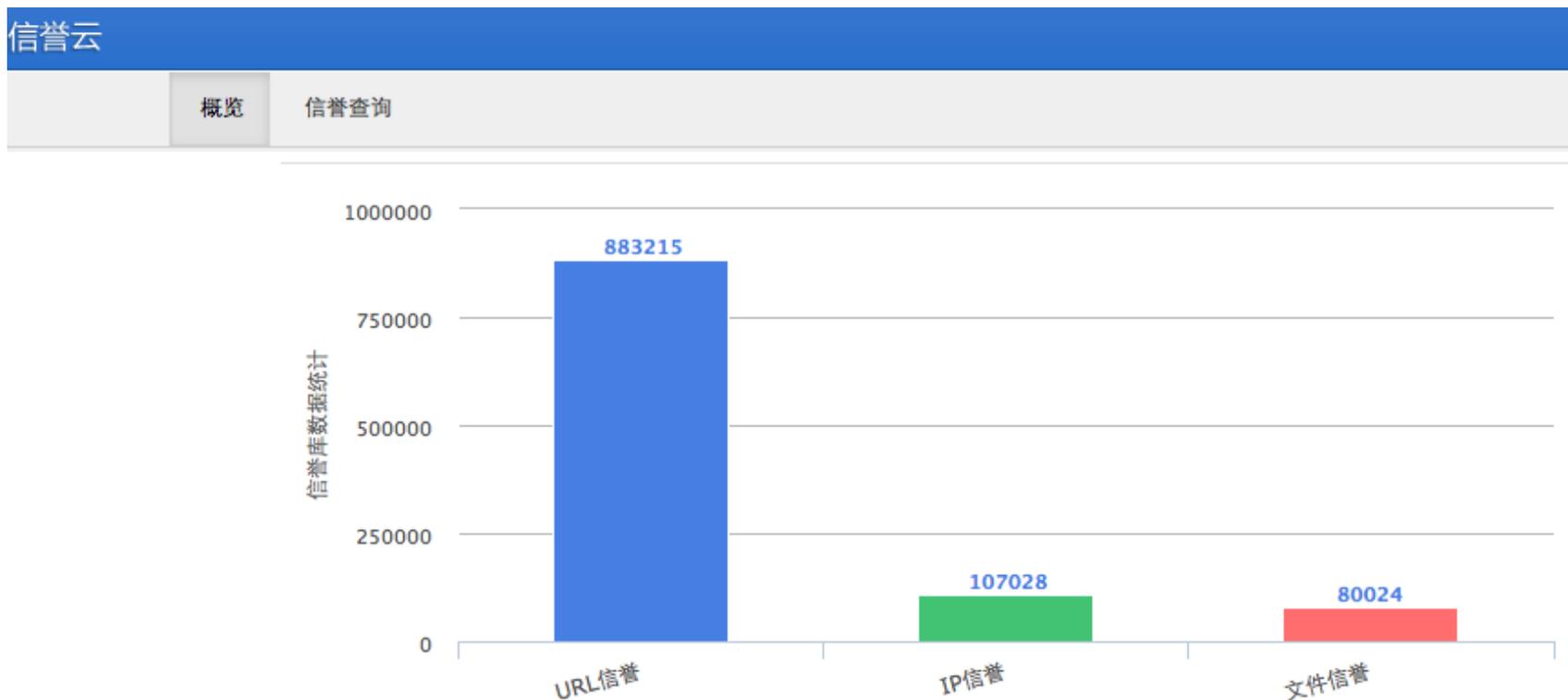
Data: 6662627063766f62686f6469666165677a78766466617364...

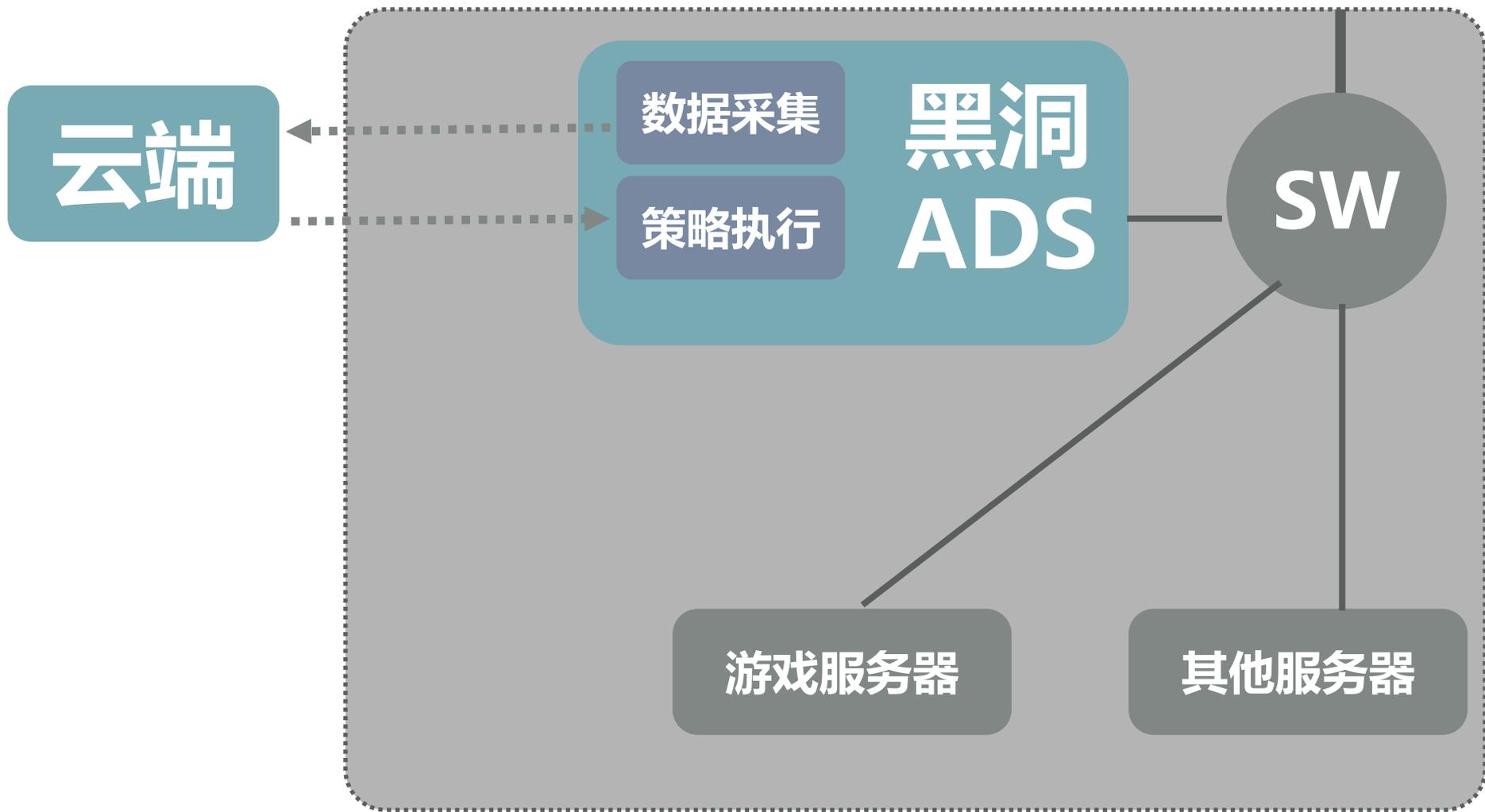
0030	ff	ff	d8	1c	00	00	66	62	62	70	63	76	6f	62	68	6ffb	bpcvobho
0040	64	69	66	61	65	67	7a	78	76	64	66	61	73	64	67	76	difaegzx	vdfasdg
0050	63	62	6e	7a	6b	6a	63	67	76	61	64	66	62	62	70	63	cbnzkjcg	vadfbbpc
0060	76	6f	62	68	6f	64	69	66	61	65	67	7a	78	76	76	61	vobhodif	aegzxvva
0070	64	66	62	62	70	63	76	6f	62	68	6f	64	69	66	61	65	dfbbpcvo	bhodifae
0080	67	7a	78	76	64	66	61	73	64	67	76	63	62	6e	7a	6b	gzxvdfas	dgvcbnzk
0090	6a	63	67	76	61	64	66	62	62	70	63	76	6f	62	68	6f	jcgvadfb	bpcvobho
00a0	64	69	66	61	65	67	7a	78	76	76	61	64	66	62	62	70	difaegzx	vvadfbbp
00b0	63	76	6f	62	68	6f	64	69	66	61	65	67	7a	78	76	64	cvobhodi	faegzxvd
00c0	66	61	73	64	67	76	63	62	6e	7a	6b	6a	63	67	76	61	fasdgvcb	nzkjcgva
00d0	64	66	62	62	70	63	76	6f	62	68	6f	64	69	66	61	65	dfbbpcvo	bhodifae
00e0	67	7a	78	76	76	61	64	66	62	62	70	63	76	6f	62	68	gzxvadf	bbpcvobh
00f0	6f	64	69	66	61	65	67	7a	78	76	64	66	61	73	64	67	odifaegz	xvdfasdg
0100	76	63	62	6e	7a	6b	6a	63	67	76	61	64	66	62	62	70	vcbnzkjc	gvadfbbp
0110	63	76	6f	62	68	6f	64	69	66	61	65	67	7a	78	76	0d	cvobhodi	faegzxv
0120	0a	63	61	6f	6e	69	6d	61	31	31	3a	20	64	66	61	73	.caonima	11: dfas
0130	64	67	76	63	62	6e	7a	6b	6a	63	67	76	61	64	66	62	dgvcbnzk	jcgvadfb
0140	62	70	63	76	6f	62	68	6f	64	69	66	61	65	67	7a	78	bpcvobho	difaegzx
0150	76	64	66	61	73	64	67	76	63	62	6e	7a	6b	6a	63	67	vdfasdg	cbnzkjcg

慧眼识金

2013年，大数据思路兴起

从海量数据中学习正常/异常的行为 精确识别异常/正常客户端





反射攻击的兴起



防御思路简单粗暴有效，关键是资源

似乎忘了说细说UDP的防御

UDP，除了DNS业务，过去一直是不被人关注的DDoS防御领域

很多客户的网络边界，甚至直接丢弃了UDP

现如今，攻击者主要发起UDP反射攻击，放大攻击流量，防护说法简单粗暴

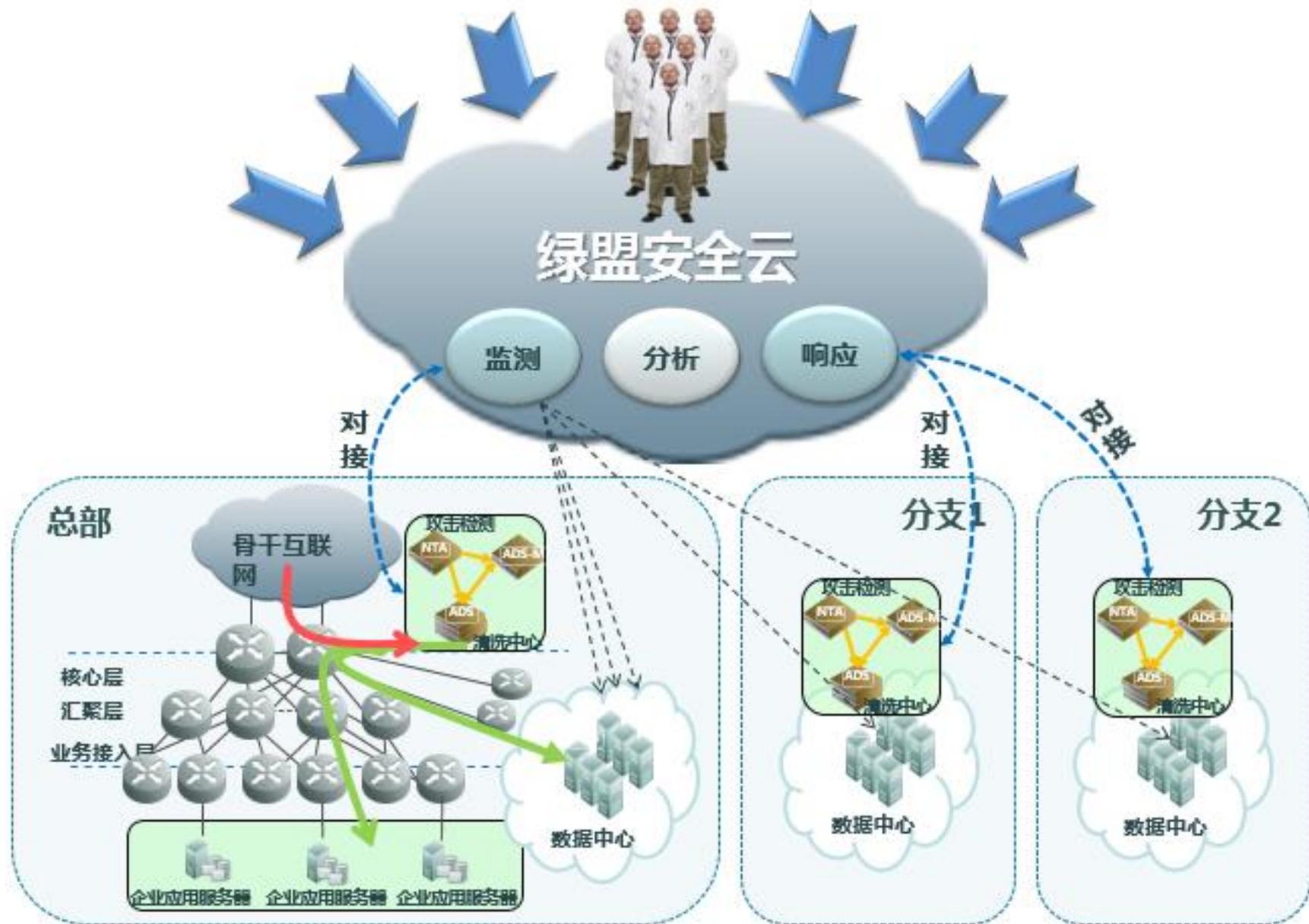
然而，我们的客户开始使用UDP跑游戏了（图片来自网络）



水印防护算法

然而不是所有的客户，都可以用水印

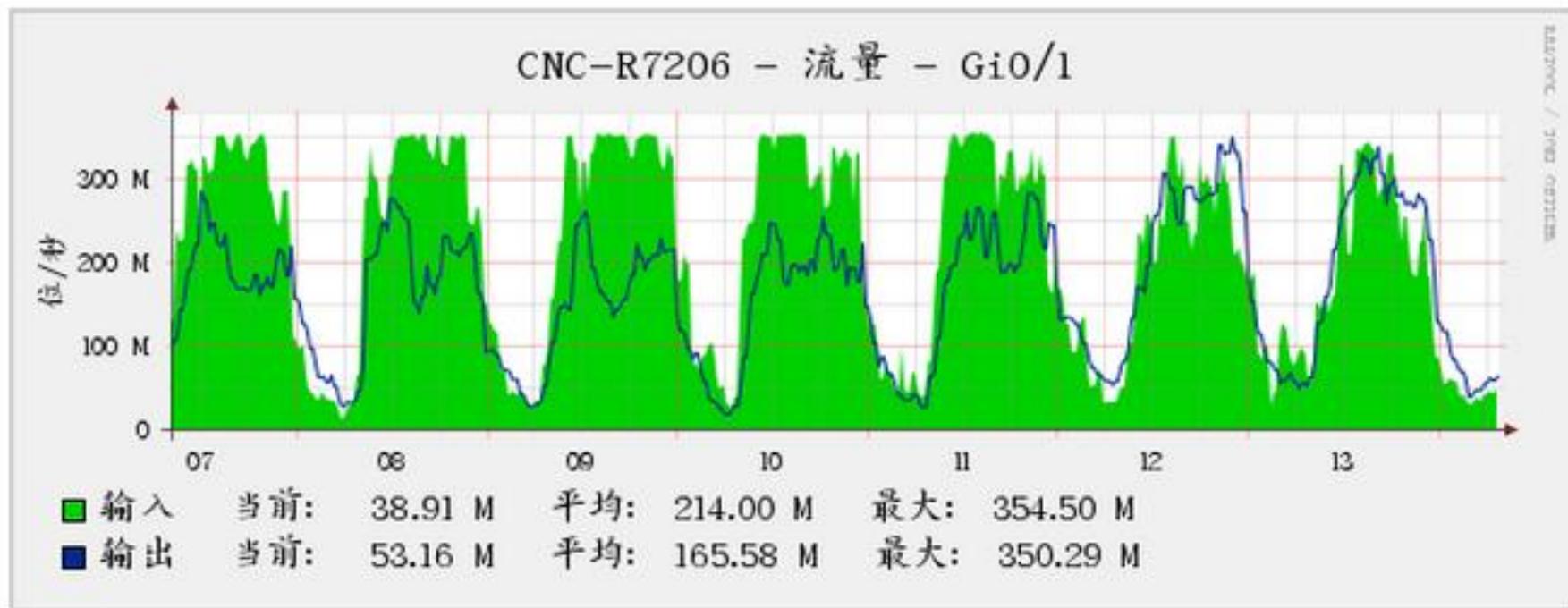
防御方案的演进



- **大部分时间在做攻击检测**
- **数据可视化**
 - **数据是否准确是第一位，否则没有可视化的意义**
 - **DDoS可视化，首先要保证极小的误报和漏报率**
- **攻击的预测和预警**

固定的告警閾值





• 业务流量不会一成不变

也总有那么些日子流量不一样，

- **双11**
- **6.18**
- **新业务上线、冲在线**
- **过年过节**

动态的阈值 + 日历策略

配置 / 监控对象 / 业务域 / 编辑IP组自学习基线-DNS_Group

返回

学习完成(已

添加



批量取消应用

SYN FLOOD

50k

时间

11月 - 11月

每月

应用阈值

25k

按日 按星期

每日

0k

11 - 11

应用 学

0:00 - 0:00

每小时

ICMP FLOOD

50k

调整倍率

320 %

应用阈值

25k

0k

应用 学

确定

取消

取消应用

bps pps



取消应用

bps pps



取消应用

bps pps



TCPFLAG

50k

— 潜伏期告警阈值(pps) ■ 流量(pps)

应用阈值

25k

确定

取消

学习过程中的异常处理

DDoS可视化 (实验室数据)



攻击事件
355



被攻击ISP
1



被攻击地区
3



被攻击业务
4

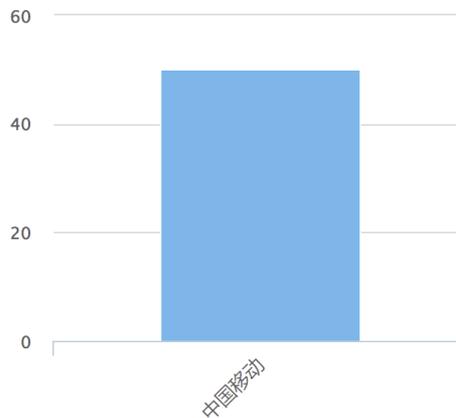
TOP5 攻击目的国家 被攻击次数



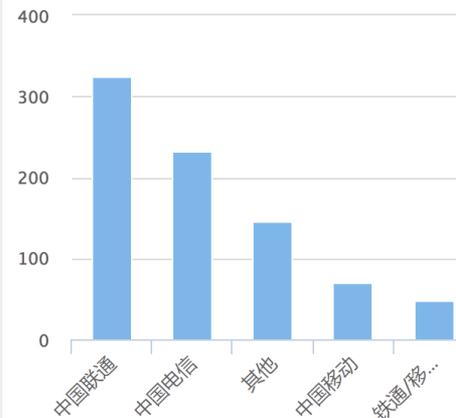
#1 美国
285

#2 中国
70

TOP5 攻击目的ISP 被攻击次数



TOP5 攻击源ISP 攻击次数





广东

报表

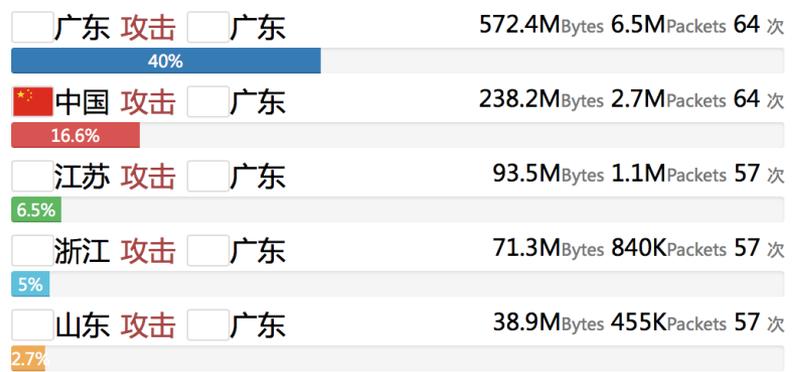
原始数据

04 TOP5 攻击地区

向本地发起攻击的地区和本地攻击的地区的TOP5排名

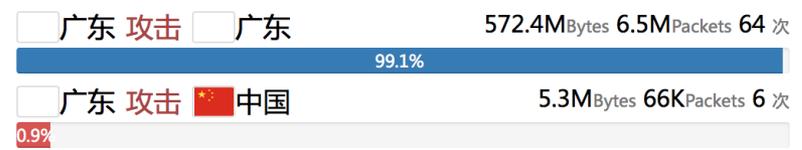
攻击源地区分布

时间内，向本地发起攻击的地区TOP5排名



攻击目的地区分布

时间内，本地攻击的地区TOP5排名



外发攻击

04 TOP5 攻击ISP

向本ISP发起攻击的ISP和本ISP攻击的ISP的TOP5排名

攻击源ISP分布

时间内，向本ISP发起攻击的ISP TOP5排名



攻击目的ISP分布

时间内，本ISP攻击的ISP TOP5排名

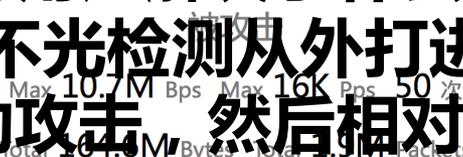


为用户解决了什么问题？

- 不光检测从外打进来的DDoS攻击，还检测从内部打出去的攻击，然后相对美观的展示出来

- 协助用户找到攻击源

- DDoS资产可视化



- **防护手段上，DDoS防护从协议验证、流量统计等思路，已开始使用大数据的思路，也确实有效**
- **排兵布阵、资源对抗上，从单点单出口防御，走向上下游协同、横纵向协同防御，DDoS不再是某一个层次就能解决问题**
- **攻击水平上，攻击者早已是集团作战，就吃这碗饭的，光脚不怕穿鞋，对防御者的资源、安全运营能力挑战极大**
- **“传统”设备接入云以获取更强的防御能力**
- **原本以为DDoS会衰减甚至消失，哪想会越来越猛**
- **攻击检测、攻击防御、攻击溯源、攻击预测**

• 做好事前准备

– 监控层面，可以监控什么？

- 流量大小、应用分布、TOPN、新建连接、并发连接、CPU负载等数据
- 正常的时候应该是什么样子

– 如果有问题，你可以找谁？

- 绿盟ADS可管理的安全服务（MSS For ADS）、ISP等

– 做好应急响应计划

建议客户做些什么？

定期进行演练

防护效果、运营能力的检阅

考虑好扩展性

负载均衡、CDN等，需要知道你的短板

做好边界防御、分层防御

关闭不必要的服务和端口，比如对于Web业务，可以封禁UDP

**虽然清洗设备可以轻松过滤反射等攻击，但仍建议将此
类DDoS防护策略靠前**

不要成为攻击源

谢谢!

关于绿盟科技

<http://www.nsfocus.com/en/>

绿盟科技是中国最早从事网络安全业务的企业之一，成立于2000年4月，总部设在中国北京，在美国硅谷、日本东京设有分支机构，在开拓北美及亚太地区的海外市场的同时，进行安全战略研究及技术预研。目前，国内的分支机构，已经遍布30余个大中型城市，为国内用户提供全面的安全服务。