



# 无中生有

基于骨干网全量应用识别的威胁情报基础数据采集

北京派网软件有限公司

## RSA总裁Amit Yoran

人们身处黑暗之中都会产生恐惧，因为当看不清周围的环境，却能听到声响或人影晃动时，人们将无法判断其中是否潜在着一些危险，这就像今天信息安全产业所面临的一个状态。



我们需要一张新的“地图”。这张“地图”一方面不依赖于预先保护机制；一方面强调普遍的可视性；一方面可以很好地进行身份认证和识别，掌握来自外部的威胁情报；一方面又能基于业务的重要级别，进行安全资源的优化部署。



威胁情报获取的难题？

# 威胁情报关键能力建设

□ 在互联网应用的推动下，从IP为实体的三层感知进化为应用为实体的七层感知，威胁情报理念发展的必然趋势。稳定的存储检索、准确的清洗、标签和关联知识库则是分析能力的基础，它们的表现直接决定了结果的有效性。

## 感知能力

应用感知

攻击感知

Session感知

IP感知

## 分析能力

关联知识库

标签知识库

清洗知识库

存储检索

# 感知有多难

**互联网触角**  
超过10万台在网设备

**识别引擎**  
现网95%以上识别率

**探针性能**  
单板40G处理能力

**部署灵活**  
通用硬件部署方便

**海量日志**  
用户、流量、事件全包括

**超细粒度**  
每P每时每刻的每个连接

# 技术链条

□ 没有互联网的飞速发展，就没有威胁情报，数据量猛增是互联网发展所带来的必然结果，准确及时的大数据分析是掌握网络运行状况和控制网络用户行为的有效手段。

数据获取

日志清洗

关联分析

客户响应

完整

准确

及时

有效

✓ 速度：超高处理性能适应互联网带宽发展趋势

✓ 广度：通达第七层，关键信息一个都不能少

✓ 内容无关：规整合并、垃圾过滤

✓ 内容相关：数据标签化、摘要常态化

✓ 存储优化

✓ 态势分析：运行状况、应用预警

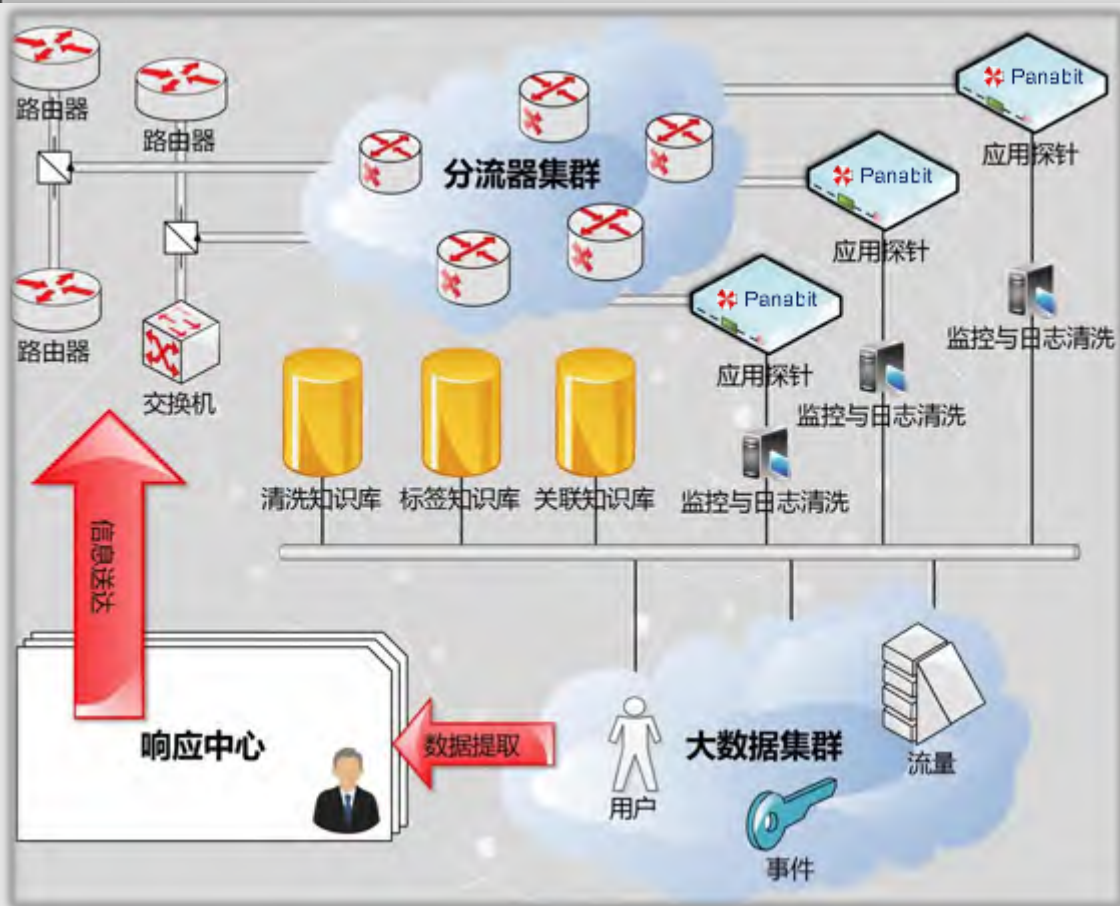
✓ 经营分析：成本利润、资源引入、聚类客户评价、潜在客户挖掘

✓ 身份定位：实体客户与网络身份映射

✓ 到达手段：上门服务、电话、短信、Web信息、微信、QQ等

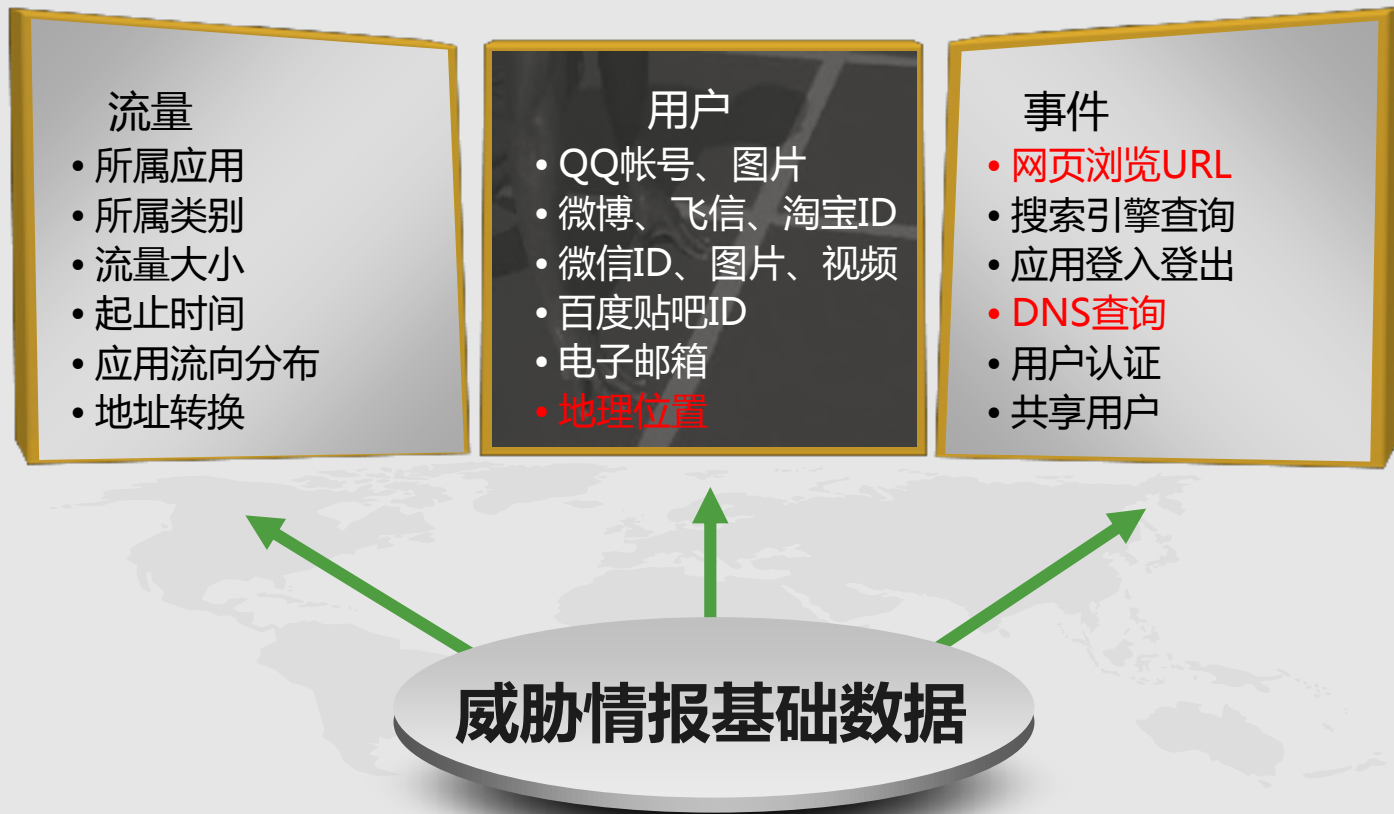


# 鸟揽威胁情报系统



- 分流子系统
  - 协议转换，同源同宿
- 探针子系统
  - 用户、事件和流量日志生成
  - 内容无关清洗
  - 数据初加工
- 知识库子系统
  - 内容相关清洗知识库
  - 标签知识库
  - 关联知识库
- 数据存储分析子系统
  - 海量存储、标签化、关联分析
- 响应子系统
  - 响应信息生成、过滤与送达

# 威胁情报源仅仅是URL和DNS？ No！





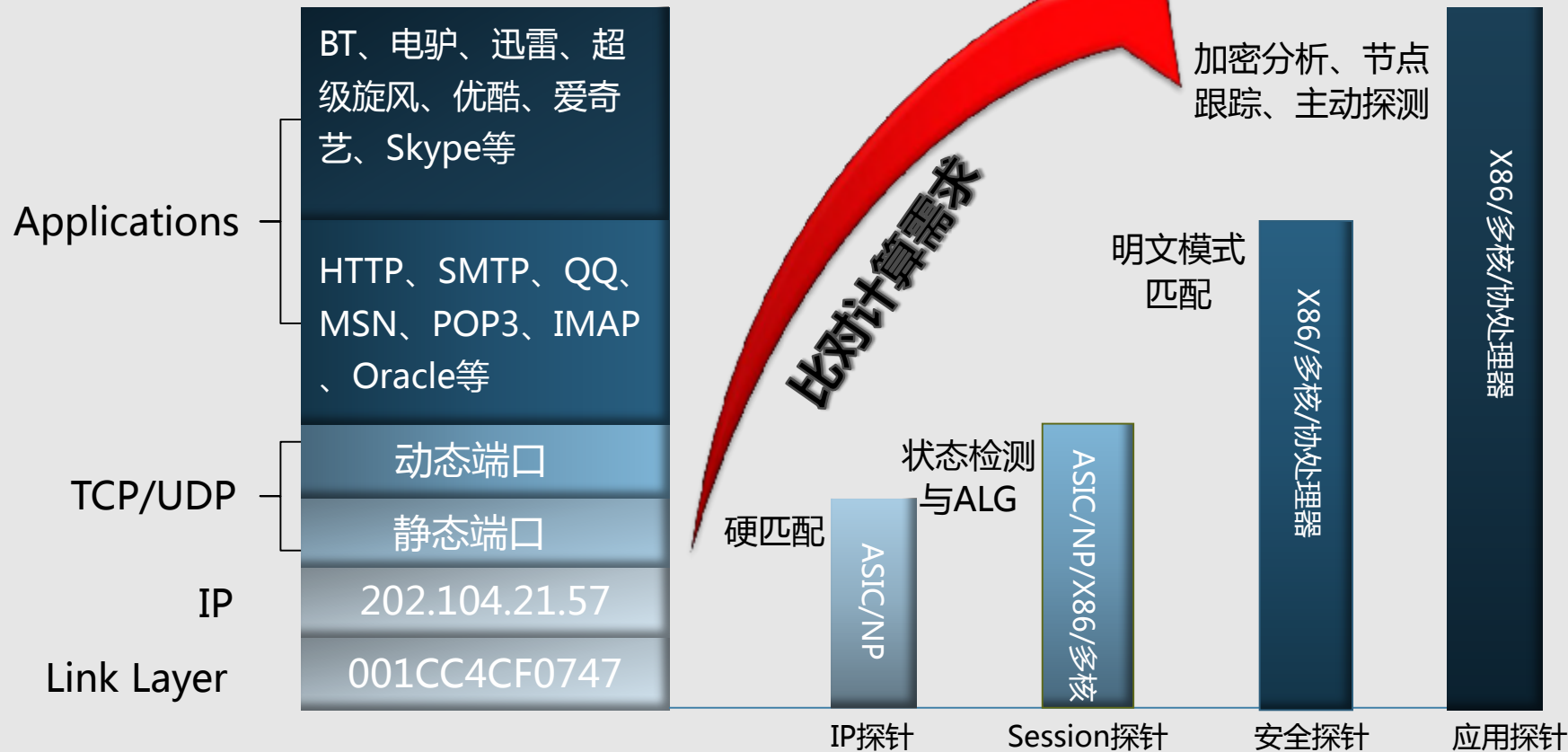
# 理想照进现实

- 记录全世界？
  - 能力对等
- 数据究竟有多大？
  - 用户、流量、事件
  - 10GE到300G字节
- 数据收敛从哪里开始？
  - 分流子系统的局限性
  - 没有数据是多余的
  - 应用探针的全流量需求
- 需要多少专家才能走完整个链条？
  - 让专业的人做专业的事
  - 通信专家、应用识别专家、大数据专家、行业知识专家



# 探针技术演进

探针设备数据面的变化



# 你是谁？

就像斯诺登所描述的一样，它游走在政府和民间的博弈中间，没人会承认，但是没人能否认它的存在。

档案->219.216.110.96					
TTL秒	在线时间(秒)	流出流量	流入流量	流出bps	流入bps
597	1229292	575.26G	847.27G	789.98K	25.28M
MAC地址		连接数	被拒绝的连接数		
00.e0.fc.46.2f.bc		2814	0/0		
序号	身份类型	身份信息	最近使用时间(s)		
1	QQ号码	1355427908	2012-09-24		
2	内部私有IP	192.168.0.91	2012-09-24		
3	QQ号码	515348695	2012-09-24		
4	POP3账号	kedadiqip@163.com	2012-09-24		
5	QQ号码	775315895	2012-09-24		
6	QQ号码	411825361	2012-09-24		

+ 防火墙日志 + 虚拟身份信息库 + IP位置信息库  
= (张三在某酒店某房间登录了某种应用)

- 为什么是Panabit？
  - 部署位置位于通信主干，无需改变连接拓扑
  - 有足够性能处理关键要素审计，不需要增加设备
  - 对应用协议分析透彻，分析协议可以涵盖邮件、即时通信、社交应用和游戏等
  - 附加移动属性：微博、微信、贴吧等

# 从哪里来？



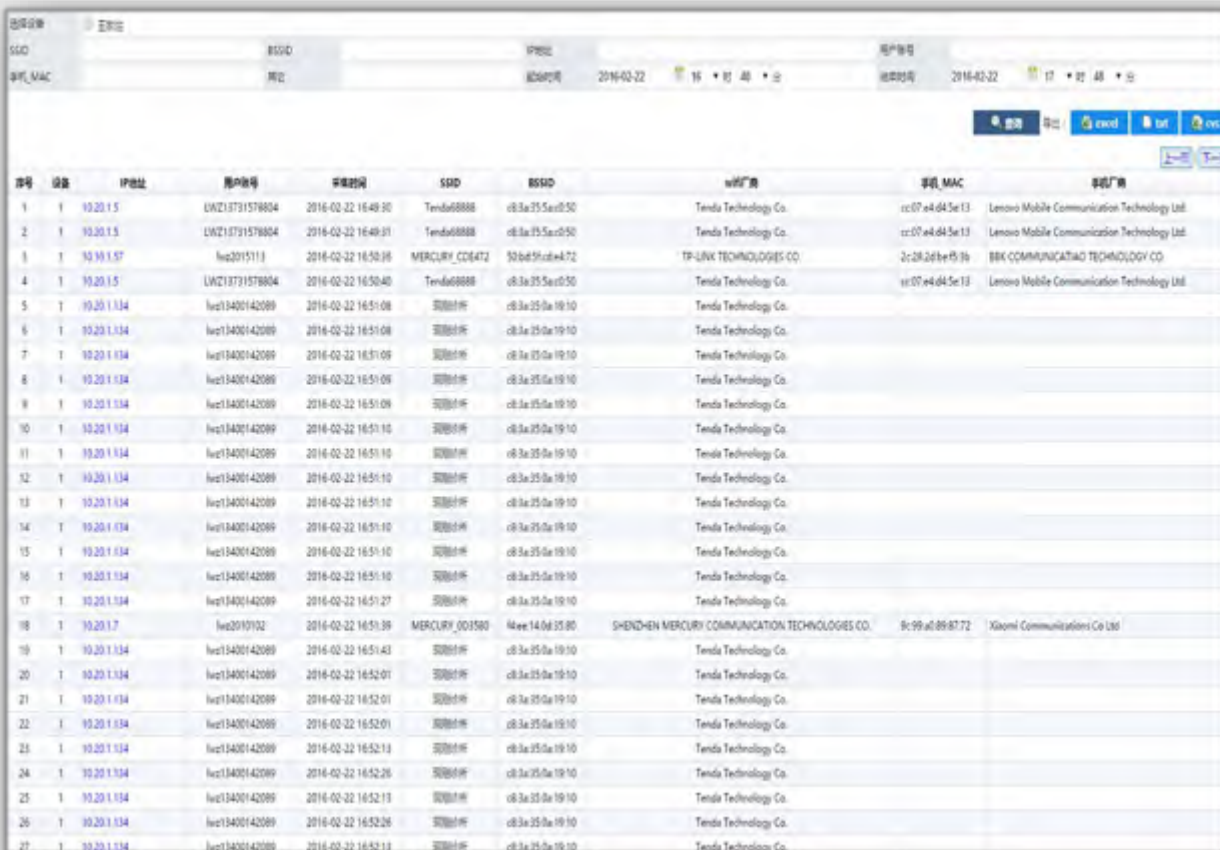
## ■ 实时精确锁定固网IP地址地理位置

- 精确度达到街道楼宇级别
- 不依赖手机移动网提供数据
- 可定位内网IP地理位置
- 噪声来源：异地访问，设备切换
- 依赖大数据统计规律

## ■ 核心用途

- 用户地理热力分析
- 应用地理热力分析
- 虚拟身份定位
- 无线环境定位
- 带宽资产核查

# 无线环境信息



序号	设备	IP地址	用户帐号	连接时间	SSID	BSSID	无线厂商	手机 MAC	手机厂商
1	1	10.20.1.5	LWZ13731578804	2016-02-22 16:49:30	Tenda68888	c8.3a.25.5a:c5.50	Tenda Technology Co.	cc:07:a4:d4:5e:13	Lenovo Mobile Communication Technology Ltd.
2	1	10.20.1.5	LWZ13731578804	2016-02-22 16:49:31	Tenda68888	c8.3a.25.5a:c5.50	Tenda Technology Co.	cc:07:a4:d4:5e:13	Lenovo Mobile Communication Technology Ltd.
3	1	10.10.1.57	hw2015711	2016-02-22 16:50:36	MERCURY_C0E472	50:b6:5f:c0:e4:72	TP-LINK TECHNOLOGIES CO.	2c:28:26:be:45:3b	BBK COMMUNICATION TECHNOLOGY CO.
4	1	10.20.1.5	LWZ13731578804	2016-02-22 16:50:40	Tenda68888	c8.3a.25.5a:c5.50	Tenda Technology Co.	cc:07:a4:d4:5e:13	Lenovo Mobile Communication Technology Ltd.
5	1	10.20.1.134	hw13400142089	2016-02-22 16:51:08	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
6	1	10.20.1.134	hw13400142089	2016-02-22 16:51:08	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
7	1	10.20.1.134	hw13400142089	2016-02-22 16:51:09	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
8	1	10.20.1.134	hw13400142089	2016-02-22 16:51:09	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
9	1	10.20.1.134	hw13400142089	2016-02-22 16:51:09	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
10	1	10.20.1.134	hw13400142089	2016-02-22 16:51:10	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
11	1	10.20.1.134	hw13400142089	2016-02-22 16:51:10	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
12	1	10.20.1.134	hw13400142089	2016-02-22 16:51:10	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
13	1	10.20.1.134	hw13400142089	2016-02-22 16:51:10	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
14	1	10.20.1.134	hw13400142089	2016-02-22 16:51:10	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
15	1	10.20.1.134	hw13400142089	2016-02-22 16:51:10	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
16	1	10.20.1.134	hw13400142089	2016-02-22 16:51:10	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
17	1	10.20.1.134	hw13400142089	2016-02-22 16:51:27	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
18	1	10.20.1.7	hw20157132	2016-02-22 16:51:39	MERCURY_003590	44ee:14:0d:35:80	SHENZHEN MERCURY COMMUNICATION TECHNOLOGIES CO.	9c:99:a0:89:87:72	Xiaomi Communications Co Ltd
19	1	10.20.1.134	hw13400142089	2016-02-22 16:51:43	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
20	1	10.20.1.134	hw13400142089	2016-02-22 16:52:01	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
21	1	10.20.1.134	hw13400142089	2016-02-22 16:52:01	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
22	1	10.20.1.134	hw13400142089	2016-02-22 16:52:01	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
23	1	10.20.1.134	hw13400142089	2016-02-22 16:52:13	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
24	1	10.20.1.134	hw13400142089	2016-02-22 16:52:26	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
25	1	10.20.1.134	hw13400142089	2016-02-22 16:52:13	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
26	1	10.20.1.134	hw13400142089	2016-02-22 16:52:26	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		
27	1	10.20.1.134	hw13400142089	2016-02-22 16:52:13	无线网卡	c8.3a.25.5a:19.10	Tenda Technology Co.		

## 无线环境

- IP和时间为索引
- 无线AP的SSID
- 无线AP的MAC地址
- 客户机MAC地址
- 无线环境探查



# 移动设备信息

The screenshot displays a web-based interface for managing mobile device information. At the top, there are search filters for 'IMEI', 'IP地址', and '用户ID'. Below the filters is a table with the following columns: '序号' (Serial Number), '设备' (Device), 'IP地址' (IP Address), '用户ID' (User ID), '采集时间' (Collection Time), 'IMEI', 'IMSI', '手机MAC' (Mobile MAC), and '手机品牌' (Mobile Brand). The table contains 37 rows of data, showing various mobile devices with their respective identifiers and collection times.

序号	设备	IP地址	用户ID	采集时间	IMEI	IMSI	手机MAC	手机品牌
1		10.20.1.4	lua2011110	2016-02-22 16:59:20	868774026113669			
2		10.20.1.119	lua2012094	2016-02-22 16:59:25	869611020027676		8473.03.6d.41.6d	
3	T	10.10.1.80	lua2019121	2016-02-22 16:59:31	86129502175365	46007811986627 中国移动	6898.67.6c.67.e0	金立 F301
4		10.20.1.119	lua2012094	2016-02-22 16:59:47	869611020027676		8473.03.6d.41.6d	
5		10.10.1.25		2016-02-22 16:59:47	860529030092895	460079300951320 中国移动	f.1a.11.2b.e9.a4	
6		10.20.1.119	lua2012094	2016-02-22 16:59:48	869611020027676		8473.03.6d.41.6d	
7		10.20.1.119	lua2012094	2016-02-22 16:59:48	869611020027676		8473.03.6d.41.6d	
8		10.20.1.119	lua2012094	2016-02-22 16:59:53	869611020027676		8473.03.6d.41.6d	
9		10.20.1.119	lua2012094	2016-02-22 16:59:55	869611020027676		8473.03.6d.41.6d	
10		10.20.1.87	lua2012090	2016-02-22 17:00:01	867786100961122	46002638678730 中国移动	481b19.bc.34.77	步步高 BBK VIVO S9
11		10.10.1.219	lua2015118	2016-02-22 17:00:39	86789602644892			Vivo Y23L
12		10.10.1.25		2016-02-22 17:00:39	860529030092895	460079300951320 中国移动	f.1a.11.2b.e9.a4	
13		10.10.1.25		2016-02-22 17:00:39	860529030092895	460079300951320 中国移动	f.1a.11.2b.e9.a4	
14		10.10.1.34	lua2012012	2016-02-22 17:01:50	866978025402173	460027139880252 中国移动		OPPO OPPO K700T
15		10.10.1.34	lua2012012	2016-02-22 17:01:50	866978025402173	460027139880252 中国移动		OPPO OPPO K700T
16		10.40.1.62		2016-02-22 17:01:50	864180202400409	46001943343330 中国移动		OPPO OPPO R800T
17		10.40.1.62		2016-02-22 17:01:50	864180202400409	46001943343330 中国移动		OPPO OPPO R800T
18		10.10.1.34	lua2012012	2016-02-22 17:01:57	866978025402173	460027139880252 中国移动		OPPO OPPO K700T
19		10.10.1.34	lua2012012	2016-02-22 17:01:58	866978025402173	460027139880252 中国移动		OPPO OPPO K700T
20		10.10.1.15	lua2019135	2016-02-22 17:02:01	862624020294090	460021119652677 中国移动		步步高 VIVO Y11
21		10.10.1.15	lua2019135	2016-02-22 17:02:01	862624020294090	460021119652677 中国移动		步步高 VIVO Y11
22		10.50.1.6	qk2014009	2016-02-22 17:02:06	86501802303888			步步高 VIVO Y22
23		10.10.1.34	lua2012012	2016-02-22 17:02:06	866978025402173	460027139880252 中国移动		OPPO OPPO K700T
24		10.10.1.34	lua2012012	2016-02-22 17:02:06	866978025402173	460027139880252 中国移动		OPPO OPPO K700T
25		10.10.1.34	lua2012012	2016-02-22 17:02:07	866978025402173	460027139880252 中国移动		OPPO OPPO K700T
26		10.10.1.34	lua2012012	2016-02-22 17:02:07	866978025402173	460027139880252 中国移动		OPPO OPPO K700T
27		10.10.1.15	lua2019135	2016-02-22 17:02:06	862624020294090	460021119652677 中国移动		步步高 VIVO Y11

## 移动设备信息

- IP和时间为索引
- IMEI：唯一标识UE硬件
- IMSI：唯一标识用户ID
- 手机MAC
- 大数据分析主要索引，例如他网手机定位



# 到哪里去？

区域流量数据分布图 (网络游戏)



## 应用去往何处？

- 所属应用：根据应用协议判定流量所属于的具体应用种类，比如：迅雷、微信、爱奇艺、魔兽世界等。
- 所属类别：归类具体应用所属的应用类别，比如：视频、即时通信、P2P下载等，目的是为了批量处理。
- 流量大小：流量所属session总数据量
- 起止时间：流量所属session开始和结束时间
- 应用流向分布：根据源地址和目的地址判别session在运营商之间或者地理版图上分布。

## 与其他业务系统的配合

- 应用镜像：根据应用复制到探针其他物理接口
- 应用路由：根据应用选择下一条路由

# 域名分布异常



## 微软威胁情报中心总经理 John Lambert

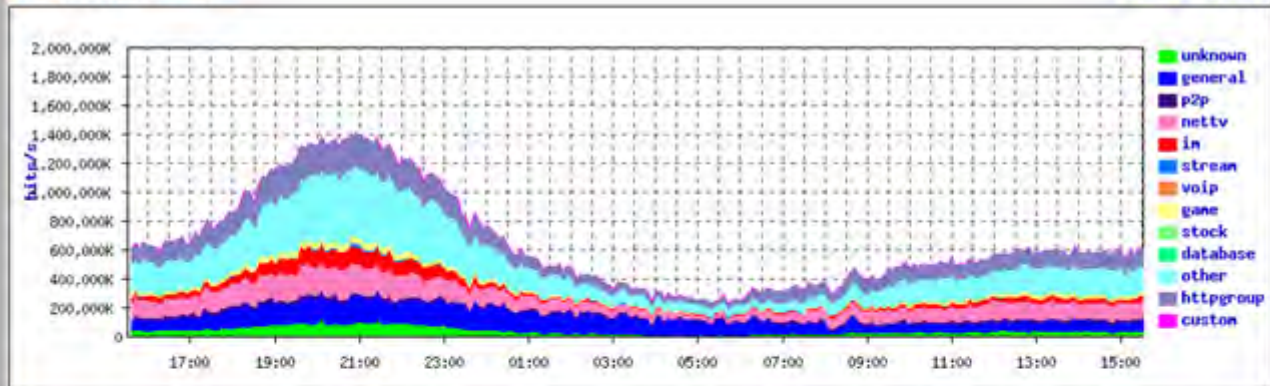
What is the most important network security spend:  
Sensor appliances? SIEM? Threat intelligence feeds?  
It's your analyst team.

**最重要的网络安全开支是什么？传感器设备？安全信息和事件管理？威胁情报来源？  
都不是，最重要的是你的分析师团队。**

# 全业务分析

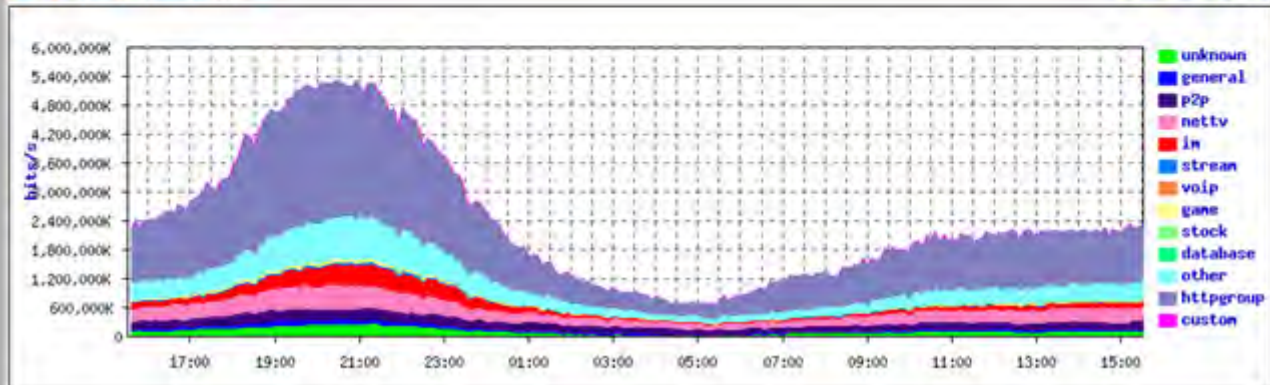
最近24小时上行流量趋势图

三日对比 历史图表



最近24小时下行流量趋势图

三日对比 历史图表



## ■ 全业务流量

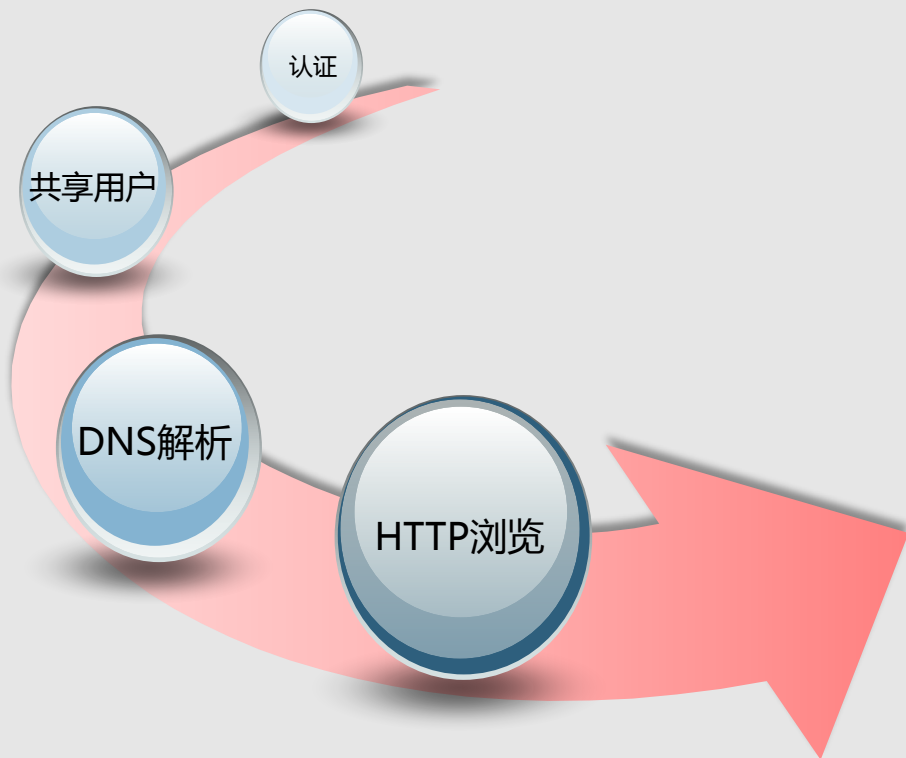
- 14大类
- 近1000种应用
- 如实反映协议完整性，从三层覆盖到七层

## ■ 可视化分析

- 分布
- 极值
- 趋势
- 相似性

## ■ 流量与事件的事件序列分析是主要未知威胁情报来源

# 时间序列分析



- HTTP浏览
  - HOST排名：发现异常，例如：病毒
  - URL分类库：判定行为，分布
  - 按IP段的URL排名：区域互联网活跃度，数据中心发展情况
- DNS解析
  - DNS解析排名：发现异常，例如：DNS Flooding，C&C
  - 时间段解析情况：应用热度
- 认证
  - 针对AAA系统的攻击与滥用
- 共享用户事件
  - 实际用户数监测：NAT后面有乾坤



# 应用画像





# 用户画像

30.20.169.109档案 已运行31天22小时32分23秒 (admin)

TTL(秒)	在线时间(秒)	流出流量	流入流量	流出bps	流入bps
591	4494	3.20M	9.63M	10.95K	54.74K
MAC地址	连接数	虚拟身份	共享用户	移动终端	
6c:9e:ed:33:00:28	21	0	0/0	无	

流量概况 **连接信息** 虚拟身份 共享用户 移动终端

红色的星经过连接数控制模块检测而被拒绝的连接

应用名称	协议	连接	WAN线路	时长	DSCP	流量(up/down)
DNS	udp	30.20.169.109:1059--180.153.162.150:53		1476	0/0	0/2071479
DNS	udp	30.20.169.109:1065--180.153.162.150:53		1476	0/0	0/2065804
DNS	udp	30.20.169.109:4278--119.167.195.3:53		1809	0/0	927582/0
DNS	udp	30.20.169.109:3087--59.46.2.109:53		940	0/0	0/172056
DNS	udp	30.20.169.109:3086--59.46.2.109:53		940	0/0	0/147288
WWW	tcp	30.20.169.109:1066--115.230.124.19:80		1233	0/0	0/94953
传奇系列	tcp	30.20.169.109:1781--117.27.240.155:8001		1601	0/0	0/5502
未知应用	tcp	30.20.169.109:4071--106.120.160.80:80		1816	0/0	235/0
未知应用	udp	30.20.169.109:4137--98.126.77.138:53		156	0/0	143/0
未知应用	tcp	30.20.169.109:1623--111.206.79.230:80		1755	0/0	134/0
SYN_ACK	tcp	30.20.169.109:1968--101.71.24.29:46539		5	0/0	0/0
SYN_ACK	tcp	30.20.169.109:2189--219.129.237.189:8885		9	0/0	0/0
传奇系列	tcp	30.20.169.109:1516--110.80.140.140:895		8	0/0	0/0
传奇系列	tcp	30.20.169.109:1503--120.41.32.238:7301		8	0/0	0/0
传奇系列	tcp	30.20.169.109:1208--120.41.32.238:7301		8	0/0	0/0
SYN_ACK	tcp	30.20.169.109:1348--101.71.24.29:46539		1	0/0	0/0
SYN_ACK	tcp	30.20.169.109:1564--113.107.181.67:7107		1	0/0	0/0
传奇系列	tcp	30.20.169.109:1535--110.80.140.140:47410		3	0/0	0/0
SYN_ACK	tcp	30.20.169.109:1348--101.71.24.29:46539		5	0/0	0/0
传奇系列	tcp	30.20.169.109:1564--113.107.181.67:7107		5	0/0	0/0
传奇系列	tcp	30.20.169.109:1535--110.80.140.140:47410		6	0/0	0/0

**重度游戏客户**

111.136.57.205档案 已运行162天17小时6分0秒 [JLCTT2]

TTL(秒)	在线时间(秒)	流出流量	流入流量	流出bps	流入bps
599	55481	1.66G	56.69G	306.50K	13.00M
MAC地址	连接数	虚拟身份	共享用户	移动终端	
00:18:82:35:3e:3c	1575	1	0/0	无	

流量概况 **连接信息** 虚拟身份 共享用户 移动终端

红色的星经过连接数控制模块检测而被拒绝的连接

应用名称	协议	连接	WAN线路	时长	DSCP	流量(up/down)
伪IE下载	tcp	111.136.57.205:60445--113.142.21.76:443		1918	0/0	535/666549331
伪IE下载	tcp	111.136.57.205:63394--113.142.13.200:443		997	0/0	535/177235011
伪IE下载	tcp	111.136.57.205:63492--113.142.13.180:443		963	0/0	1072/174987935
伪IE下载	tcp	111.136.57.205:65398--123.138.162.97:443		138	0/0	487/68025556
QQ聊天	udp	111.136.57.205:52946--111.161.88.90:8000		39775	0/0	157092/903396
QQ聊天	udp	111.136.57.205:29929--113.142.10.71:8000		39664	0/0	125952/34506
超级拨号	udp	111.136.57.205:29909--58.39.230.117:29909		4782	0/0	127452/0
迅雷	udp	111.136.57.205:14759--112.65.1.104:15473		2677	0/0	28528/0
迅雷	udp	111.136.57.205:14759--112.65.1.104:15473		2476	0/0	26387/0
迅雷	udp	111.136.57.205:14759--112.65.1.104:15473		2476	0/0	25279/0
迅雷	udp	111.136.57.205:14759--123.139.176.174:28418		2350	0/0	25255/0
迅雷	udp	111.136.57.205:14759--112.65.1.104:15473		2470	0/0	23499/0

**重度下载客户**

# 应用画像与用户画像交叉引用

← → ↻ <https://58.30.71.38/index.htm>



系统维护 应用识别 应用路由 PPPOE服务 策略管理 **实时监控**

系统概况->Top应用

已运行2009

网桥 所有流量 按照 连接数 排序 显示前 30 项 隔 不刷新 秒刷新

协议名称	连接数	上行bps	下行bps	代理上行bps	代理下行bps
DNS	2579524	361.18K	8.37M	0	0
PPWeb	113531	11.76M	9.98M	10.01M	10.26M
WWW	54716	26.48M	153.16M	15.54M	123.22M
eDonkey	20293		86.05K	243.00K	84.84K
未知应用	1941		5.70M	129.76K	400.50K
SYNACK	8776	2.00M	924.9K	1.24M	653.25K
Bittorrent	8345	11.57M	16.10M	4.36M	12.95M
Skype	7930	303.89K	305.56K	17.14K	16.58K
迅雷	7335	51.84M	31.52M	44.30M	27.35M
微信聊天	5290	892.18K	8.20M	718.20K	7.65M
360更新	4548	2.10M	1.24M	1.50M	712.10K
酷狗	4092	201.99K	10.00M	126.73K	7.85M
QQ直播	3986	226.77K	740.78K	224.63K	739.06K
大唐宽带	3961	9.20K	16.30K	5.82K	9.58K
PPLive	2538	418.18K	1.23M	185.27K	1.21M
未知80端口	2536	45.97K	101.06K	39.50K	72.54K

区区8M数据，瞬间击垮一个二级运营商出口

58.30.110.130档案

已运行200天7小时37分37秒 (歌华A0机房crash过)

TTL(秒)	在线时间(秒)	流出流量	流入流量	流出bps	流入bps
598	11318505	1.58G	2.51G	2.30K	3.74K
MAC地址	连接数	虚拟身份	共享用户	移动终端	
00:22:93:61:00:89	985	0	0/0	无	

流量概况 连接信息 虚拟身份 共享用户 移动终端

红色的是经过连接数控制模块检测而被拒绝的连接

应用名称	协议	连接	WAN线路	时长	DSCP	流量(up/down)
DNS	udp	58.30.110.130:53--89.72.132.156:13614		186	0/0	0/53
DNS	udp	58.30.110.130:53--119.177.182.34:41862		144	0/0	0/53
DNS	udp	58.30.110.130:53--97.68.78.55:3777		39	0/0	0/53
DNS	udp	58.30.110.130:53--4.175.170.27:45433		144	0/0	0/53
DNS	udp	58.30.110.130:53--117.58.252.0:58742		155	0/0	0/53
DNS	udp	58.30.110.130:53--76.155.93.137:62655		46	0/0	0/53
DNS	udp	58.30.110.130:53--19.108.19.5:14301		35	0/0	0/53
DNS	udp	58.30.110.130:53--118.215.28.160:2128		73	0/0	0/53
DNS	udp	58.30.110.130:53--46.216.109.77:51453		135	0/0	0/53
DNS	udp	58.30.110.130:53--5.251.26.114:9320		107	0/0	0/53
DNS	udp	58.30.110.130:53--84.136.158.94:17776		36	0/0	0/53
DNS	udp	58.30.110.130:53--97.246.237.153:44935		73	0/0	0/53
DNS	udp	58.30.110.130:53--5.197.125.74:34516		166	0/0	0/53
DNS	udp	58.30.110.130:53--117.75.216.48:49352		138	0/0	0/53
DNS	udp	58.30.110.130:53--117.151.40.204:4604		109	0/0	0/53
DNS	udp	58.30.110.130:53--77.81.98.93:18080		177	0/0	0/53
DNS	udp	58.30.110.130:53--85.245.244.71:40499		114	0/0	0/53
DNS	udp	58.30.110.130:53--57.200.193.22:12968		114	0/0	0/53
DNS	udp	58.30.110.130:53--123.211.114.189:26725		143	0/0	0/53
DNS	udp	58.30.110.130:53--120.99.19.31:487		25	0/0	0/53
DNS	udp	58.30.110.130:53--119.126.135.172:29866		143	0/0	0/53



# 极值实例-网站排名分析

序号	域名	访问数	上行流量	下行流量
1	mmsns.qqpic.cn	71946	6.29G	88.04G
2	market.huobi.com	68888	45.85M	1.06M
3	wa.gting.com	68888	45.85M	1.06M
4	www.22mt.la	68888	45.85M	1.06M
5	116.211.111.250	68888	45.85M	1.06M
6	www.sqmai.cn	15069	2.46M	1.36M
7	mobads-logs.baidu.com	43508	496.7M	42.68M
8	short.weixin.qq.com	31830	12.64G	6.09G
9	sango.qzone.qqzoneapp.com	48676	67.57M	270.16M
10	bbs.eduwest.com	48154	2.19M	2.89M
11	tieba.baidu.com	105111	1.01G	2.18G
12	appstore.duokanbox.com	56520	13.3M	5.44M
13	monitor.uu.qq.com	79537	4.23G	783.22M
14	3g.music.qq.com	90704	33.6M	6.17M
15	news.sina.com.cn	116733	70.57M	109.62M
16	mvads.kugou.com	60686	82.89M	1.13M
17	api.chat.xiaomi.net	56079	537.13M	140.06M
18	msg.api.xiaoenai.com	21114	1.05M	158.65K
19	qzonestyle.gting.cn	107903	1.35G	5.07G
20	dl28.yunpan.360.cn	41210	48.08M	10.26G
21	182.118.24.33	51465	2.8M	11M
22	caoimg.com	66842	8.55M	335.6M

区域流量 --> 宁夏

序号	域名	访问量	上行流量(Byte)	下行流量(Byte)	总流量(Byte)
1	vi0.6.cn	65524	1.06M	0	1.06M
2	www.download.windowsupdate.com	65013	46.44M	683.7M	730.14M
3	www.hx2car.com	64584	5.48M	586.94K	6.05M
4	portal.maxthonimg.com	64503	331.74K	2.69M	3.02M
5	vr5.6rooms.com	63842	1.09M	0	1.09M
6	assets.dvstatic.com	62475	28.37M	83.52M	111.89M
7	jebe.xnimg.cn	61106	2.57M	21.3M	23.87M
8	www.doniv.net	60133	604.57K	644.68K	1.22M
9	sp.vip.com	59956	2.39M	38.39M	40.78M
10	cc.acgvideo.com	58486	5.22M	15.52G	15.52G
11	vi0.6.cn	55572	1.04M	0	1.04M
12	cu005.www.duba.net	55323	53.9M	2.77G	2.82G
13	vi0.6rooms.com	54561	1.24M	0	1.24M
14	vj6.6rooms.com	54492	901.38K	0	901.38K
15	snapshot.file.yy.com	54310	519.85K	652.42K	1.14M
16	screenshot.dvstatic.com	53736	9.34M	67.15M	76.49M
17	share.vip.com	53029	10.96M	3.91M	14.87M
18	image.yy.com	52973	143.42M	1.43G	1.57G
19	p0.pstatp.com	52609	1.49M	10.46M	11.95M
20	static.myy.com	52484	101.57M	475.66M	577.22M
21	i0.6.cn	52081	1.05M	0	1.05M
22	vj0.6rooms.com	51763	5.26M	29.5M	34.76M
23	ax.init.itunes.apple.com	51005	6.79M	29.22M	36.01M
24	s1.doyo.cn	50874	8.87M	31.66M	40.54M
25	img2a0bi.com	48414	1.71M	7.98M	9.7M
26	uploadmp3.6rooms.com	48375	973.59K	90.87M	91.82M
27	s.cimg.163.com	47824	77.76M	490.86M	568.62M
28	123.94.26.134	47568	5.61M	1.94G	1.95G

批量推动微软升级，  
产生的直接效果



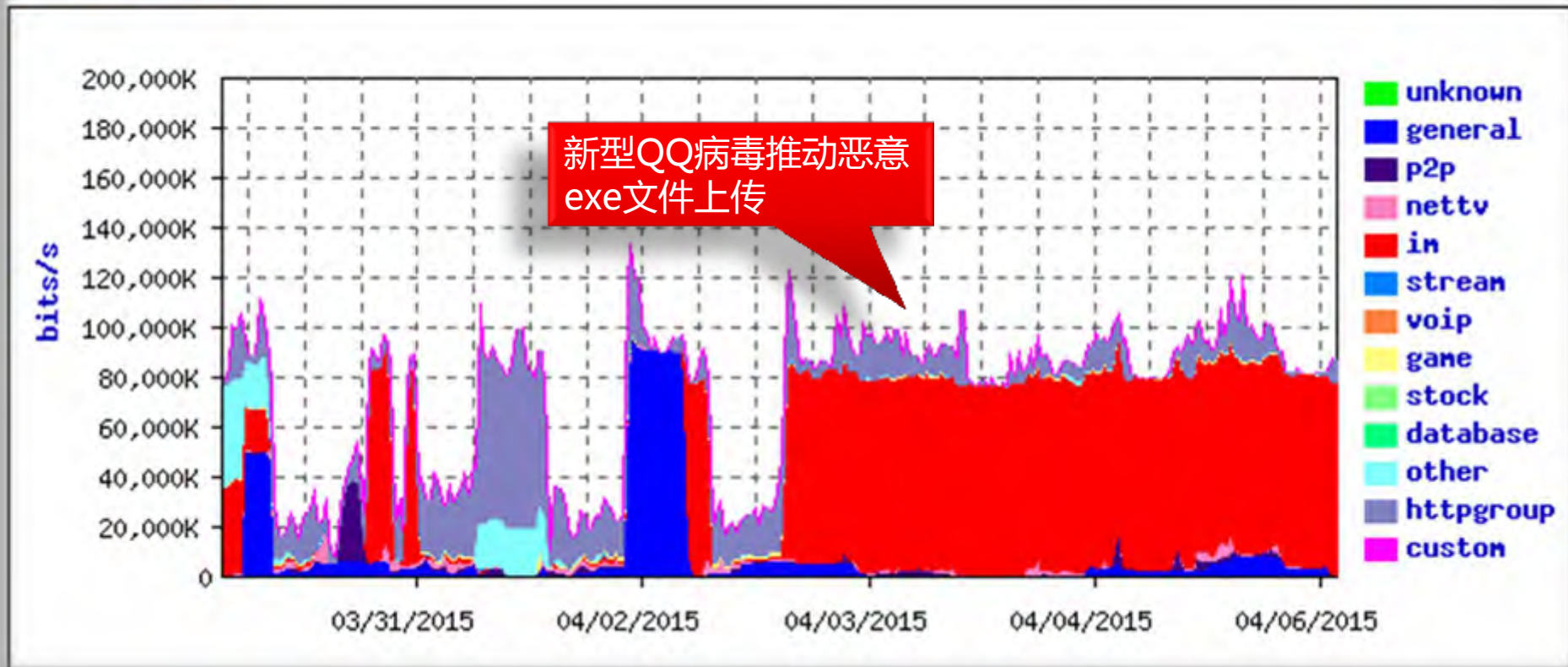
# 极值实例- App安全的那些梗

序号	域名	访问次数	上行流量	下行流量	总流量	操作
1	monitor.uu.qq.com	1881584	5.52G	3.51G	9.03G	
2	loc.map.baidu.com	1766395	10.82G	5.36G	16.18G	
3	mmsns.qpic.cn	1759599				
4	configsvr.msfn3g.qq.com	1701188				
5	inews.gtimg.com	1695213				
6	sdk.open.phone.igexin.com	1619056				
7	adash.m.taobao.com	1610455				
8	dc.51y5.net	1607358				
9	click.hd.sohu.com.cn	1585586				
10	irs01.com	1581510				
11	rqd.uu.qq.com	1575842				
12	ma.3g.qq.com	1571284				
13	mobads-logs.baidu.com	1556379				
14	igtimg.cn	1542240				
15	msg.71.am	1470466				
16	mbdlog.iqiyi.com	1429592				
17	dlied1.qq.com	1383214				
18	omgmta.qq.com	1377206				
19	wx.qlogo.cn	1374550				
20	android.bugly.qq.com	1348349				

```
"st" = "m"  
"uhid" = "a0000000000000000000000000000001"  
"dcType" = "005021"  
"sign" = "D57843D62EF602EC0A0F3036EFB5FDD7"  
"pid" = "00500101"  
"msg" = "{"cts":"1467819787260","aid":"42a188baff4dce4"}"  
"capBssid" = "14:e6:e4:d6:ba:9a"  
"mac" = "00:9a:cd:ad:17:ea"  
"mapSP" = "a"  
"verName" = "4.1.28"  
"userToken" = ""  
"verCode" = "3058"  
"appId" = "A0008"  
"netModel" = "w"  
"capSsid" = "yang1"  
"chanId" = "guanwangn160704"  
"ts" = "1467819788123"  
"lati" = "25.312966"  
"longi" = "110.306319"  
"imei" = "A00000592EC4CE"  
"dhid" = "f074429347df42c88581bd16a172bfe3"  
"lang" = "cn"  
"origChanId" = "guanwangn160704"
```

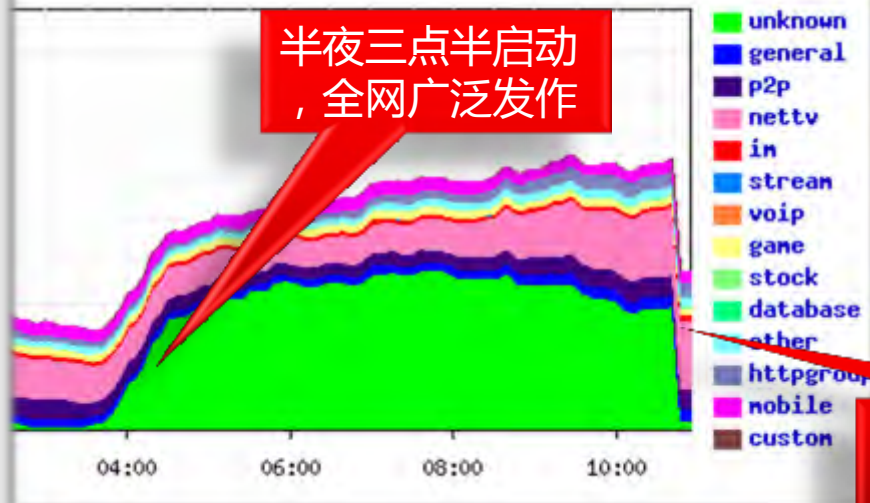
# 趋势实例-QQ空间病毒

最近1周趋势图



# 分布实例-磊科蠕虫事件

半夜三点半启动，全网广泛发作



集中攻击UDP 53413端口的未知流量

115.120.58.212档案

TTL(秒)	在线时间(秒)	流出流量	流
592	60489	2.61G	

MAC地址	连接数	流
e4.c7.22.2e.0e.c6	79472	0/0

应用名称	协议	连接	AN线路	时长	DSCP	流量 (up/down)
未知应用	udp	115.120.58.212:12837--123.52.91.37:53413		40	0/0	225/30
未知应用	udp	115.120.58.212:12837--193.185.53413		124	0/0	225/0
未知应用	udp	115.120.58.212:12837--193.84.53:53413		173	0/0	225/0
未知应用	udp	115.120.58.212:12837--193.166:53413		103	0/0	225/0
未知应用	udp	115.120.58.212:12837--193.84.52:53413		173	0/0	225/0
未知应用	udp	115.120.58.212:19949--61.26.223.191:53413		92	0/0	225/0
未知应用	udp	115.120.58.212:30122--157.113.140.238:53413		50	0/0	225/0
未知应用	udp	115.120.58.212:32300--154.120.9.164:53413		103	0/0	225/0
未知应用	udp	115.120.58.212:30121--157.113.140.237:53413		50	0/0	225/0
未知应用	udp	115.120.58.212:32301--154.120.9.165:53413		103	0/0	225/0
未知应用	udp	115.120.58.212:17222--7.42.91.131:53413		159	0/0	225/0
未知应用	udp	115.120.58.212:9304--2.95.203.211:53413		28	0/0	225/0
未知应用	udp	115.120.58.212:11922--105.101.181.43:53413		1	0/0	225/0

在Panabit协助下，中国互联网11:00启动全网封堵

## 磊科 (NetCore) 全系列路由器中的“疑似后门”程序

2014-12-31 +10 共188368人围观,发现32个不明物体 网络安全 资讯

看近年来的路由器后门，多数是内网...  
等，再有就是存在一些很明显的“漏洞”...  
太说不过去了.....这些功能是不是有点...  
针对磊科路由器2014年的一个漏洞的蠕虫集中爆发



# 相似性实例-真假DNS

The image shows a screenshot of the Panabit network analysis tool. The top part displays traffic statistics for various protocols, with a red box highlighting the '相对集中的目标地址分布' (Relative concentration of target address distribution) for DNS. Below this, a table lists traffic details with columns for '序号' (Serial Number), '设备' (Device), '协议名称' (Protocol Name), '协议' (Protocol), '源时间' (Source Time), '目标时间' (Destination Time), '源地址' (Source Address), '源端口' (Source Port), '目标地址' (Destination Address), '目标端口' (Destination Port), '名称' (Name), '流量' (Traffic), and '设备' (Device). A red box points to the '目标地址' column, noting '什么时候53端口也变成了未知?' (When did port 53 also become unknown?).

The bottom part of the image shows a packet capture analysis. A red box highlights a '畸形的UDP 53端口原始数据包' (Distorted original UDP packet on port 53). The packet details show a DNS Zone change notification. The 'Expert Info' section indicates a 'Malformed Packet' error.

序号	设备	协议名称	协议	源时间	目标时间	源地址	源端口	目标地址	目标端口	名称	流量	设备
3	10	未知应用	TCP	2015/12/09 12:24:44	11	10.93.111.77	5503	104.237.141.130	53		1174 / 512	其它
3	10	未知应用	UDP	2015/12/09 12:23:40	0	19.70.192.325	53924	220.181.127.61	53		10 / 73	电话
3	10	未知应用	UDP	2015/12/09 12:23:00	0	10.77.86.32	27375	220.181.127.65	53		10 / 73	电话
4	10	未知应用	UDP	2015/12/09 12:23:00	0	10.129.13.202	56420	111.161.99.109	53		270 / 240	普通
5	10	未知应用	UDP	2015/12/09 12:23:00	0	19.91.20.61	29311	218.35.117.57	53		758 / 46	普通
6	10	未知应用	UDP	2015/12/09 12:23:00	0	10.93.102.101	60611	220.181.127.69	53		762 / 220	电话
7	10	未知应用	UDP	2015/12/09 12:23:00	0	10.72.33.109	27752	108.120.167.10	53		10 / 73	电话
8	10	未知应用	UDP	2015/12/09 12:23:00	0	10.82.56.196	93984	111.206.255.255	53		798 / 662	普通

No.	Time	Source	Destination	Protocol	
2	1.145967	00:da:81:d3:b7:01	111.206.62.168	Broadcast	who has 172.26.1.230
3	1.692558	172.26.1.230	111.206.62.168	DNS	Standard query
4	1.803570	111.206.62.168	172.26.1.230	DNS	Standard query
5	2.778244	172.26.1.230	172.26.1.230	DNS	Standard query
6	2.787387	123.125.80.73	172.26.1.230	DNS	Standard query
7	3.418959	169.254.174.18	169.254.255.255	NBNS	Name query NB C
8	3.990756	172.26.1.230	111.206.62.215	DNS	Standard query
9	4.186217	169.254.174.18	169.254.255.255	NBNS	Name query NB C
10	4.936440	169.254.174.18	169.254.255.255	NBNS	Name query NB C
11	6.107737	172.26.1.230	111.206.62.168	DNS	Standard query
12	6.972119	172.26.1.01	111.206.60.48	DNS	Standard query
13	8.964724	169.254.174.18	169.254.255.255	NBNS	Name query NB W
14	8.998639	172.26.1.223	111.206.62.215	DNS	Standard query
15	9.014010	111.206.62.215	172.26.1.221	DNS	Standard query

相对集中的目标地址分布

什么时候53端口也变成了未知?

畸形的UDP 53端口原始数据包

```
13 5.208121 172.20.0.38 111.206.62.168 DNS Zone change notification Unknown (11188) • Unknown extended lib • (Malformed)
M Frame 12: 898 bytes on wire (7168 bits), 898 bytes captured (7188 bits) on interface 0
E Ethernet II, Src: e0:2b:ca:19:0c:40 (e0:2b:ca:19:0c:40), Dst: 00:0d:8c:1d:07:03 (00:0d:8c:1d:07:03)
P PPP-over-Ethernet Session
P Point-to-Point Protocol
P Banner protocol, Src: 172.26.0.11 (172.26.0.11), Dst: 111.206.62.168 (111.206.62.168)
P User Datagram Protocol, Src Port: 50144-mux (1029), Dst Port: 53 (53)
P Internet Name System (query)
I Malformed packet: dns
[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
[Message: Malformed Packet (Exception occurred)]
[Severity Level: Error]
[Group: Malformed]
```

```
udp53.txt 记事本
文件(F) 编辑(E) 格式(O) 帮助(H)
1 111.206.62.168
2 111.206.62.168
3 111.206.62.168
4 111.206.62.168
5 111.206.62.168
6 111.206.62.168
7 111.206.62.168
8 111.206.62.168
9 111.206.62.168
10 111.206.62.168
11 111.206.62.168
12 111.206.62.168
13 111.206.62.168
14 111.206.62.168
15 111.206.62.168
16 111.206.62.168
17 111.206.62.168
18 111.206.62.168
19 111.206.62.168
20 111.206.62.168
```

# 全程开放策略



探针可以根据数据类型，以标准格式输出日志信息到PanaLog或者任何第三方接收平台。

Panabit运行的PANAOS操作系统可以加载第三方APP，在保证性能和稳定性前提下扩展探针功能。

PanaLog预制大数据接口，可在监控清洗基础上，将需要的日志输出到后端大数据平台。



**Panabit**