DDoS攻击的分布式协同防御

龚俭
东南大学计算机科学与工程学院
CERNET华东北地区网络中心
2015.11.24

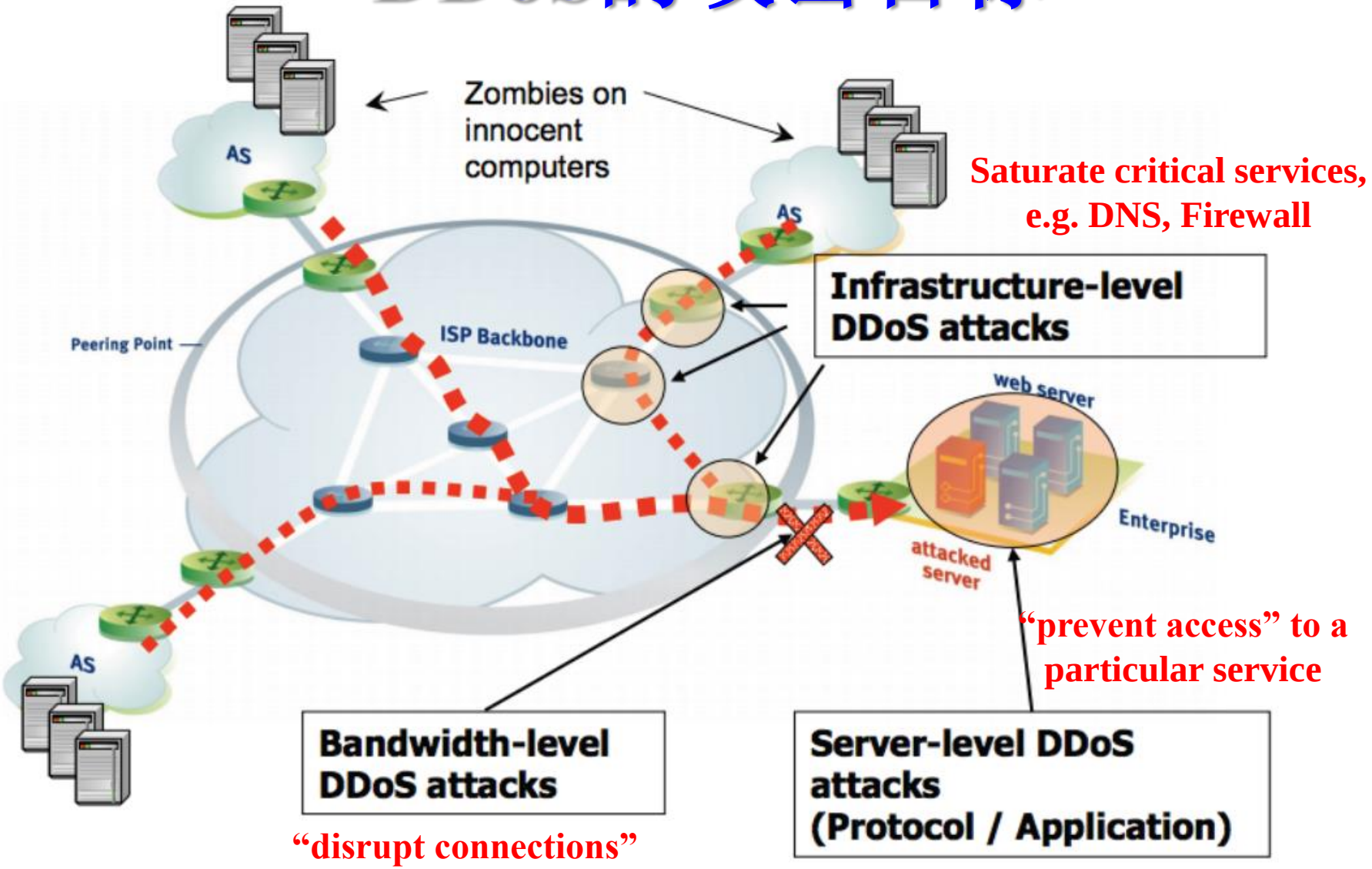
大纲

- 主干网安全的研究热点
- **DDoS攻击**
- **DDoS监测**
- **DDoS防御**
- **Hydra系统**

HSARPA的网络空间安全战略研究计划

- **Research Theme 3：Network Security**
  - **Security Protections for DNS**
  - **Security Protocols for the Routing Infrastructure**
  - **Next-Generation DDoS Defense：大规模，溯源**
  - **Network Measurement and Mapping：Enrich**
  - **Modeling of Internet Attacks：恶意代码行为**
  - **Network Reputation and Risk Analysis：风险管理**

DDoS的攻击目标

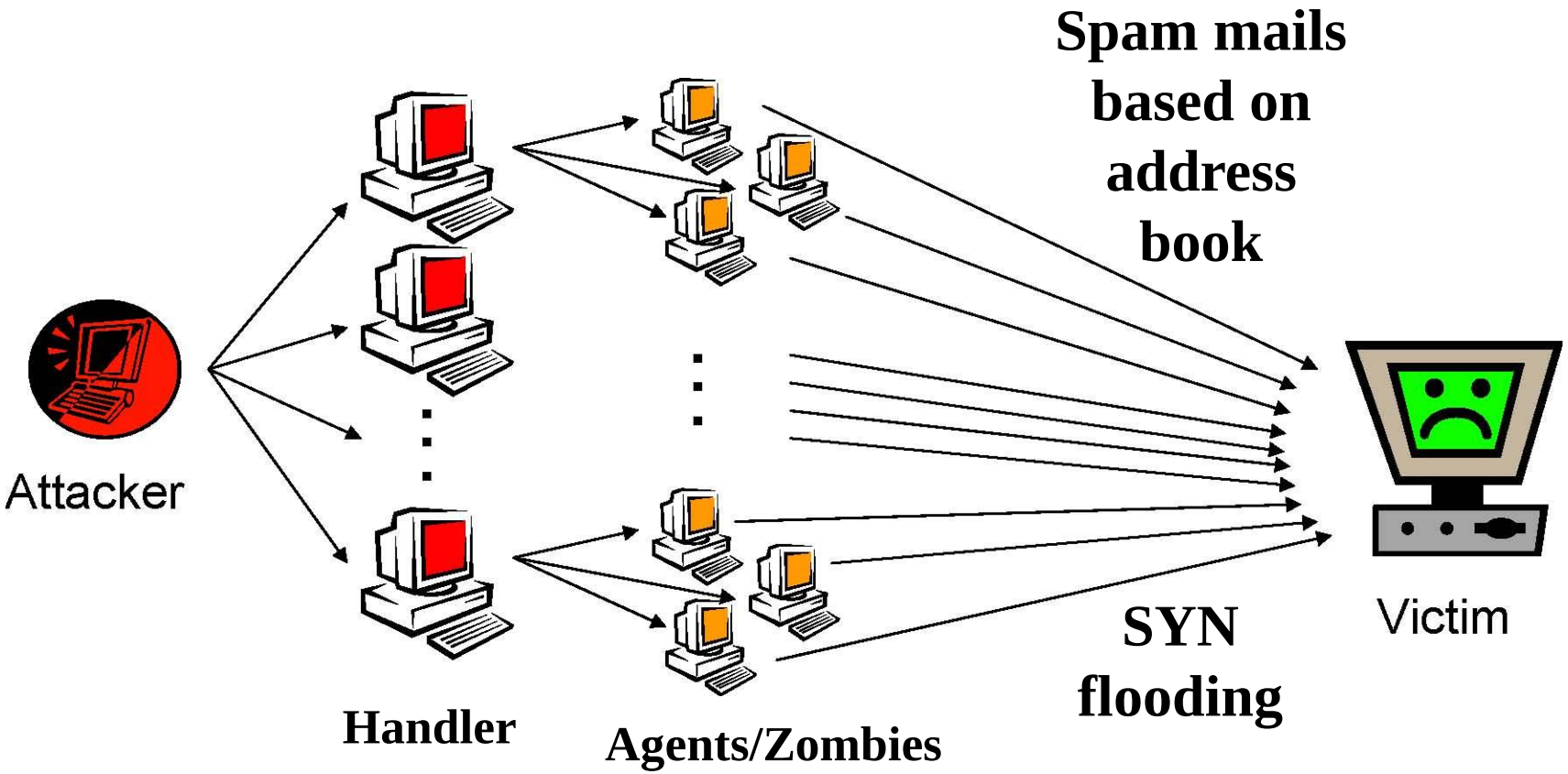


Saturate critical services, e.g. DNS, Firewall

"prevent access" to a particular service

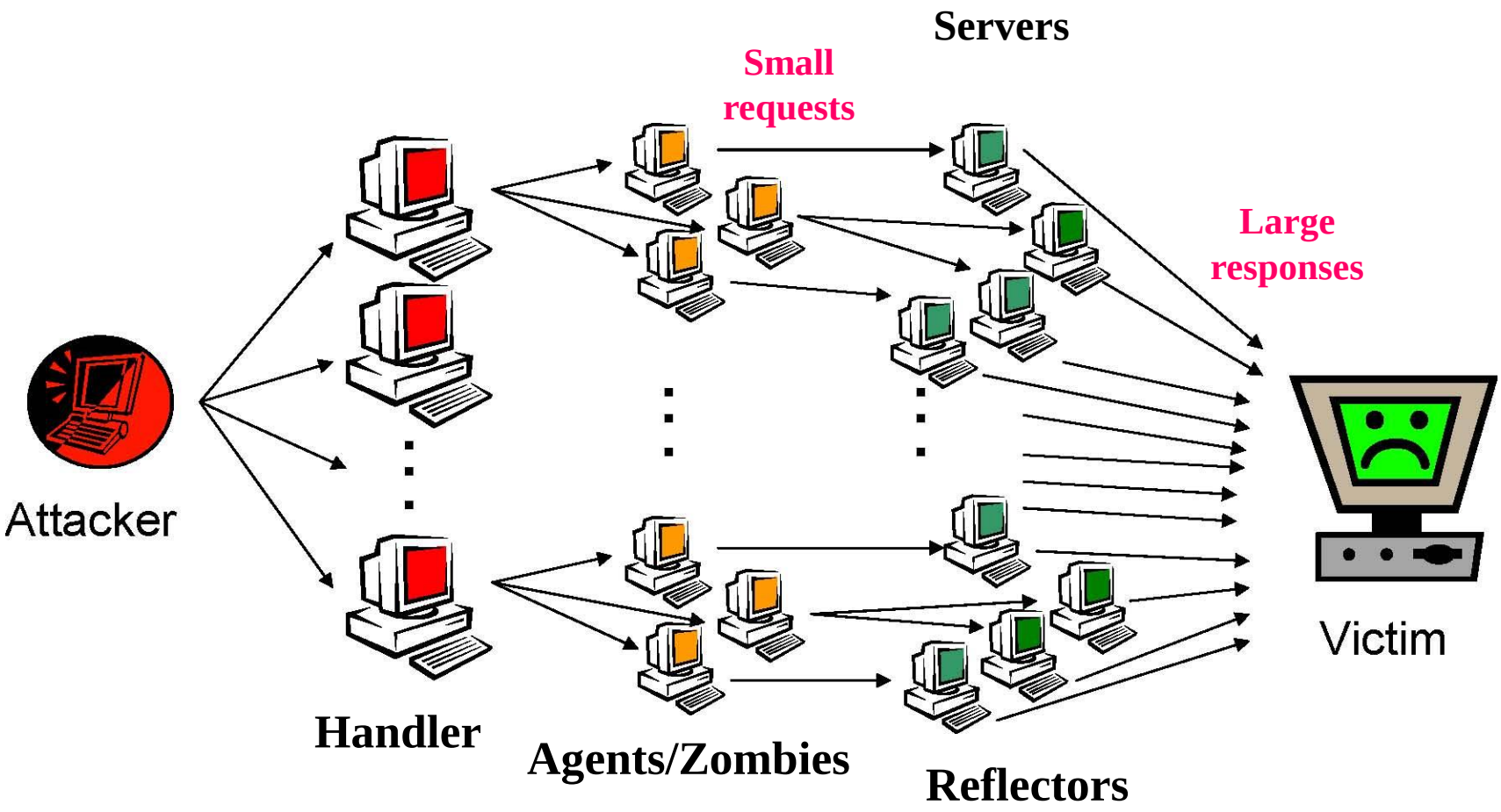
"disrupt connections" between two networks

DDoS的攻击放大



用于直接DDoS攻击的放大网络

分布式反射服务失效攻击DRDoS



DRDoS

- 特点
  - 攻击者的隐蔽性-被攻击者收到的是放大器发送的散射流量，攻击者的标识被隐藏；
  - 攻击源的广泛性-攻击者可同时使用多个放大器，使得在一个上行信道上产生广泛分布的攻击流量；
  - 显著的倍增性-被攻击者收到的攻击流量远大于攻击者发送给放大器的流量。
- 可用于DRDoS的协议具有下列特征
  - 请求与响应之间存在明显的流量差；**bps或pps**
  - 不需要或没有恰当的握手机制，因此可以源冒充。

协议放大率分析

Protocol	BAF *all*	BAF 50%	BAF 10%	PAF *all*	Scenario
SNMP v2	6.3	8.6	11.3	1.00	*GetBulk* request
NTP	556.9	1083.2	4670.0	10.61	Request "monlist" statistics
DNS_{NS}	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS_{OR}	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	*SEARCH* request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Sality	37.3	37.9	38.4	1.00	URL list exchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

$$BAF = \frac{len(UDP\ payload)\ amplifier\ to\ victim}{len(UDP\ payload)\ attacker\ to\ amplifier} \qquad PAF = \frac{number\ of\ packets\ amplifier\ to\ victim}{number\ of\ packets\ attacker\ to\ amplifier}$$

Amplification Hell: Revisiting Network Protocols for DDoS Abuse
Christian Rossow， NDSS '14, 23-26 February 2014, San Diego, CA, USA

协议放大器调查

Protocol	Amplifiers	Tech.	t_{1k}	t_{100k}
SNMP v2	4,832,000	Scan	1.5s	148.9s
NTP	1,451,000	Scan	2.0s	195.1s
DNS_{NS}	255,819	Crawl	35.3s	3530.0s
DNS_{OR}	7,782,000	Scan	0.9s	92.5s
NetBios	2,108,000	Scan	3.4s	341.5s
SSDP	3,704,000	Scan	1.9s	193.5s
CharGen	89,000	Scan	80.6s	n/a
QOTD	32,000	Scan	228.2s	n/a
BitTorrent	5,066,635	Crawl	0.9s	63.6s
Kad	232,012	Crawl	0.9s	108.0s
Quake 3	1,059	Master	0.6s	n/a
Steam	167,886	Master	1.3s	137.1s
ZAv2	27,939	Crawl	1.5s	n/a
Sality	12,714	Crawl	4.7s	n/a
Gameover	2,023	Crawl	168.5s	n/a

Amplification Hell: Revisiting Network Protocols for DDoS Abuse
Christian Rossow， NDSS ’14, 23-26 February 2014, San Diego, CA, USA

Arbor的调查结果-普遍性

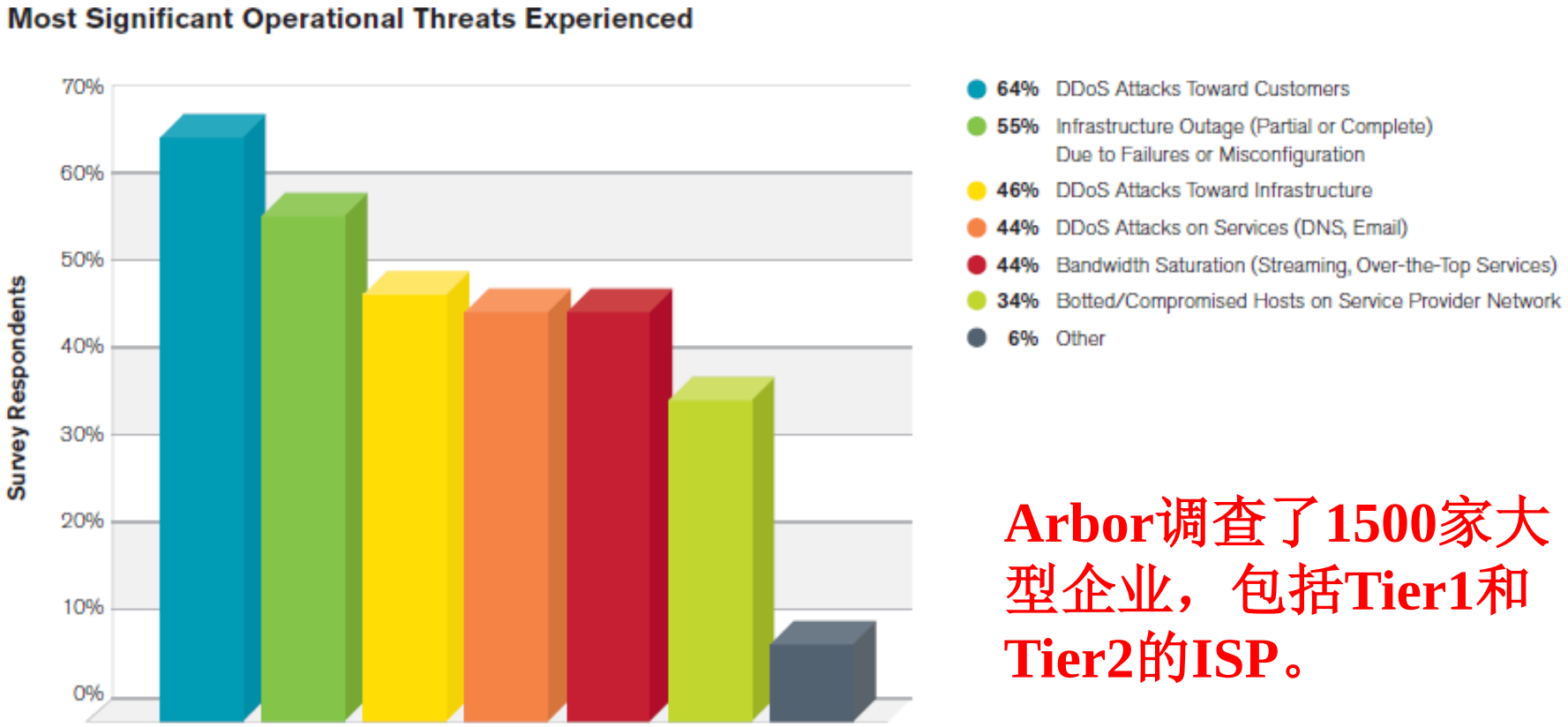


Figure 10 Source: Arbor Networks, Inc.

Arbor调查了1500家大型企业，包括Tier1和Tier2的ISP。

The report provides the results of Arbor Network's ninth annual Worldwide Infrastructure Security Survey. The survey covers a 12-month period from Nov. 2012 through the end of Oct. 2013. This report documents the collective experiences, observations and concerns of the operational security community in 2013.

Arbor的调查结果-动机

Most Common Motivations Behind DDoS Attacks

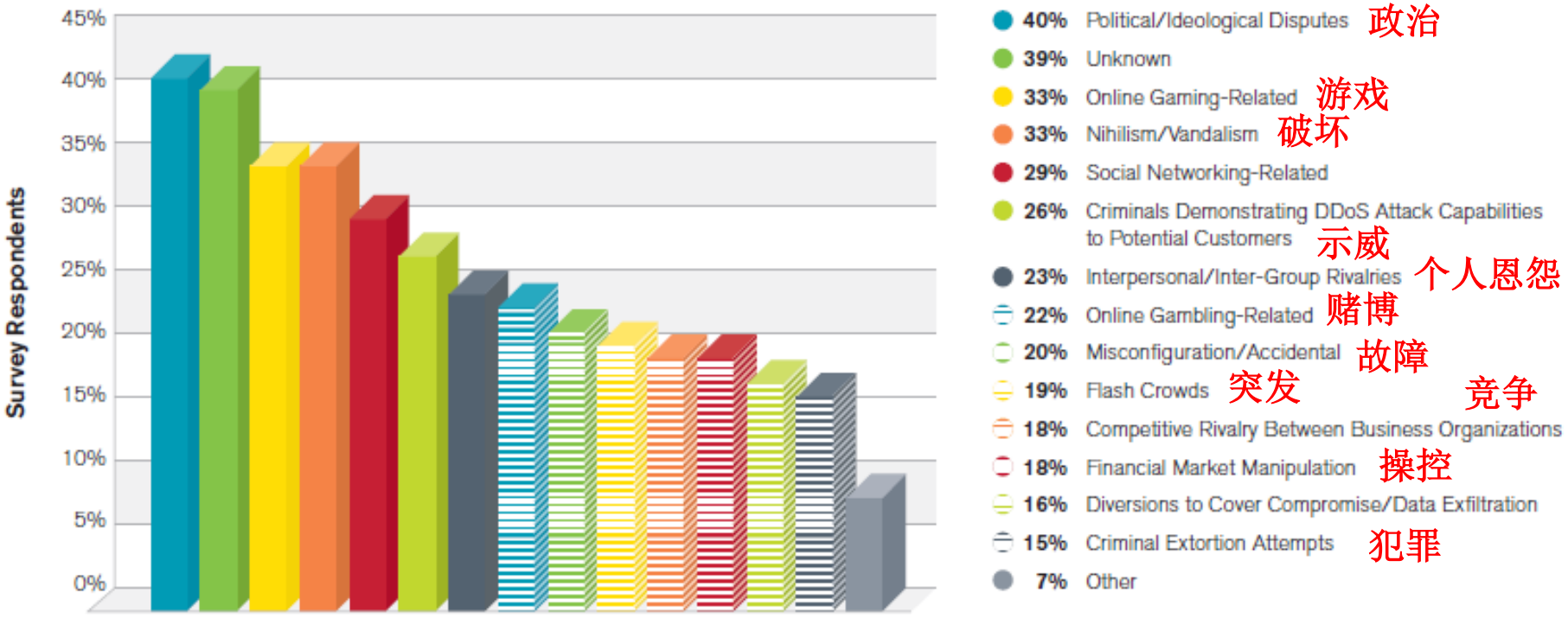
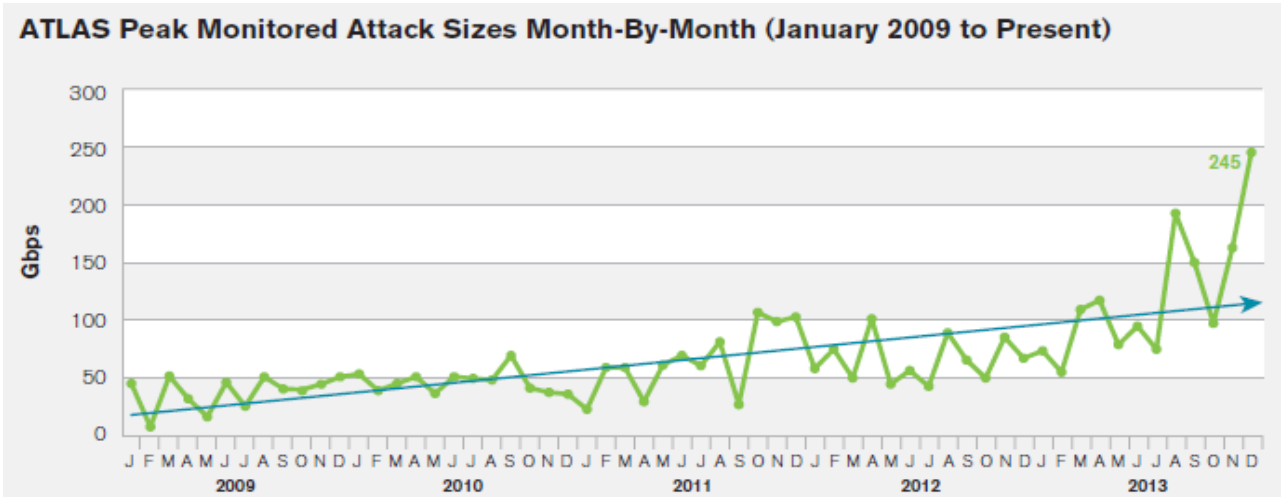


Figure 13 *Source: Arbor Networks, Inc.*

Arbor的调查结果-强度



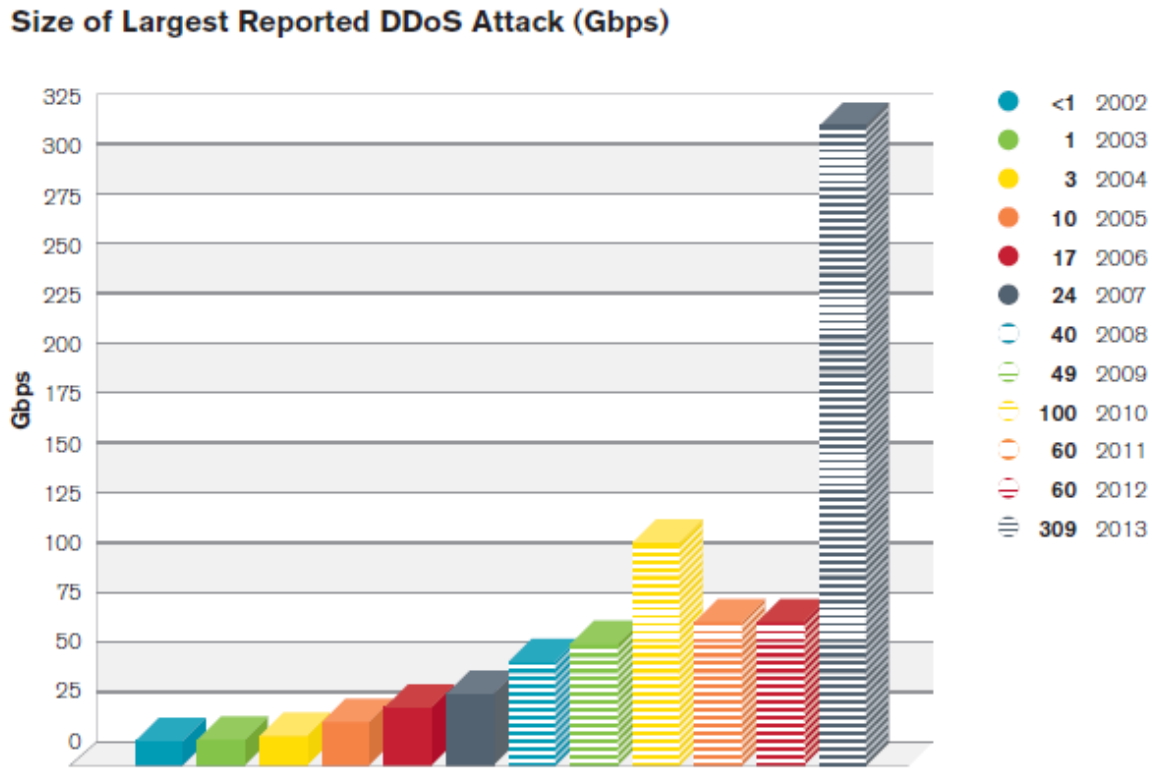


Figure 14 Source: Arbor Networks, Inc.

The targets of these largest reported attacks of over 100Gbps have all been UDP/53 or TCP/80, or the combination of both of these.

Duration of Largest DDoS Attack

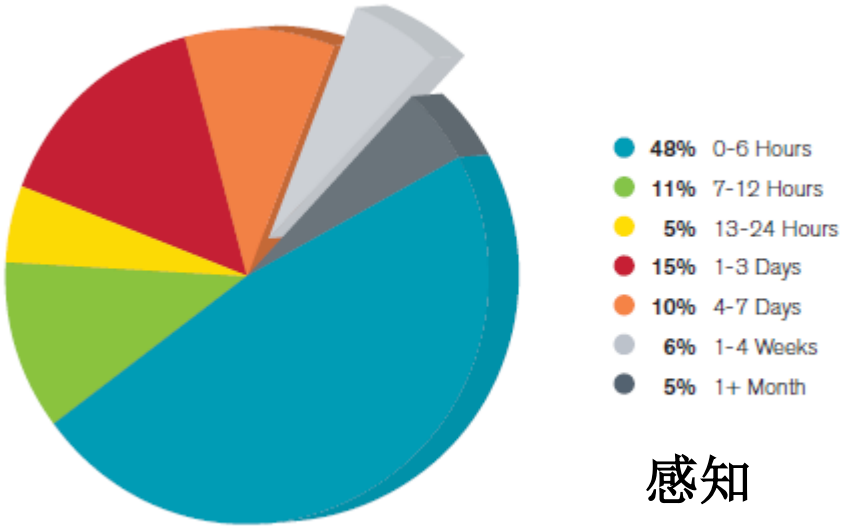


Figure 17 Source: Arbor Networks, Inc.

Target of Largest DDoS Attack

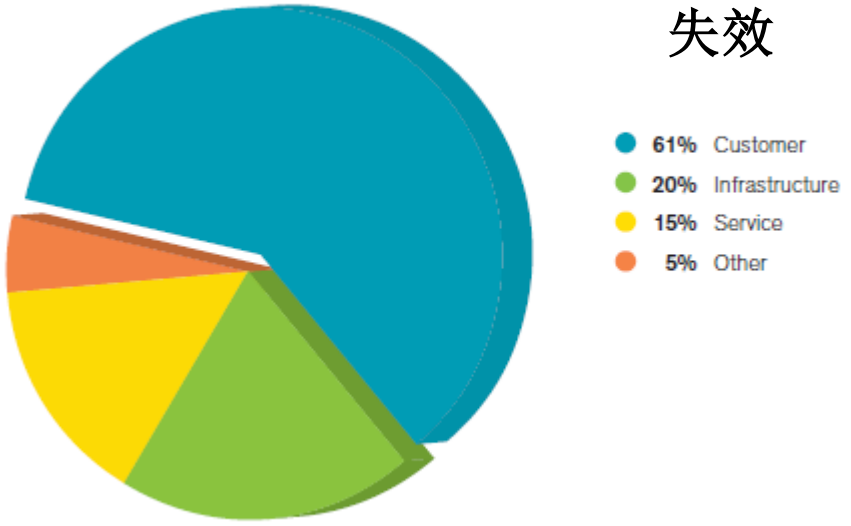


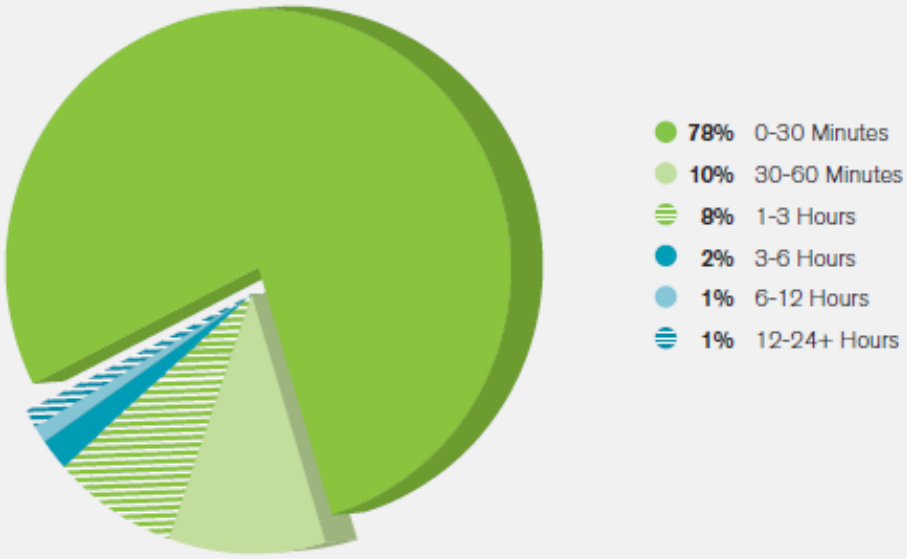
Figure 18 Source: Arbor Networks, Inc.

感知

影响

失效

ATLAS-Monitored Attack Durations



ATLAS-Monitored Volumetric Service Targets

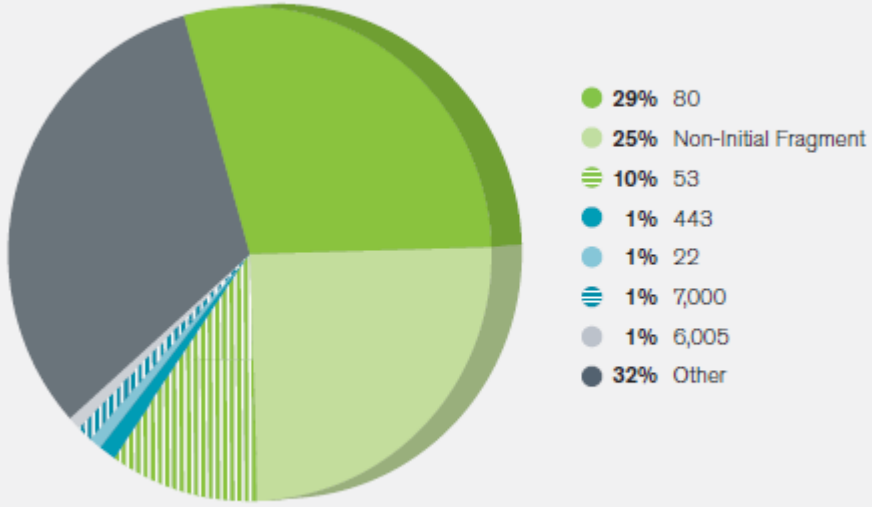


Figure 25 Source: Arbor Networks, Inc.

新动向

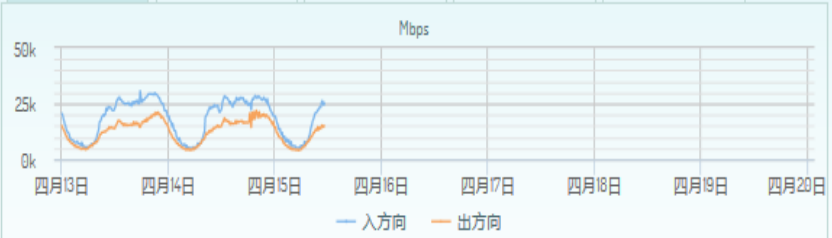
- **2014年12月20-21号，阿里云计算宣布遭到14小时的DDoS攻击，峰值强度达到453.8Gb/s;**
- **2014年9月，一个由1.2万-1.5万个由无线AP、家用恒温器、烘干机等物联网设备构成的僵尸网络在亚洲和美国发起了多次DDoS攻击，峰值强度达到215Gb/s;**
- **2014年，江苏基础电信企业的DNS服务器被由无线AP、视频监控设备和机顶盒设备构成的僵尸网络实施泛查询攻击，强度达到400万QPS。**

NBOSv3.0

首页 基本流量行为 服务质量 热点检测 安全威胁分析 其他 CHAIRS系统 2.0版

本周被管网流量 More...

总体 | 教育网 | 国内 | 国际 | 其它



【入方向】最大：30765.04 Mbps； 平均：18187.10 Mbps
【出方向】最大：22081.64 Mbps； 平均：12391.98 Mbps

【入方向】最大：8505.81 Kpps； 平均：3053.74 Kpps
【出方向】最大：5412.11 Kpps； 平均：2252.92 Kpps

带宽占用

被管单位	出/入带宽(Mbps)
	3252/4786
CERNET华东	4506/1866
南京	1639/2207
南	377/3066
南京	405/1191
江苏有线数据	578/775
南京	218/997
江苏云港	442/686
南京	99/889
CERNET南京	580/282
南京	153/665
中国	388/428

应用分布

应用名	流量比例(%)
WWW	65.81
P2P	18.62
Skype	4.89
其它语音	0.02
系统端口	1.44
IBR	0.09
邮件	0.41
交互	0.91
数据库	0.04
FTP	<0.01
DNS	0.16
其它	7.60

当前网内有反射攻击行为的主机 More...

IP	归属	端口	总流量(MB)	次数	首次检出时间	末次检出时间
211.87.34.166	职业大学	19	874746.64	4924	2015-03-31 14:18:46	2015-04-15 11:13:26
219.219.75.223	大学	19	347299.50	1817	2015-03-24 14:53:52	2015-04-15 11:13:23
219.219.218.18	中国	123	52001.90	2068	2015-04-10 16:53:07	2015-04-15 11:12:27
219.219.218.16	中国	123	54756.94	2163	2015-04-10 16:53:13	2015-04-15 11:12:21
202.119.199.155	大学	123	49425265.95	89455	2015-02-01 19:13:38	2015-04-15 11:12:13

最近DDoS攻击检测 More...

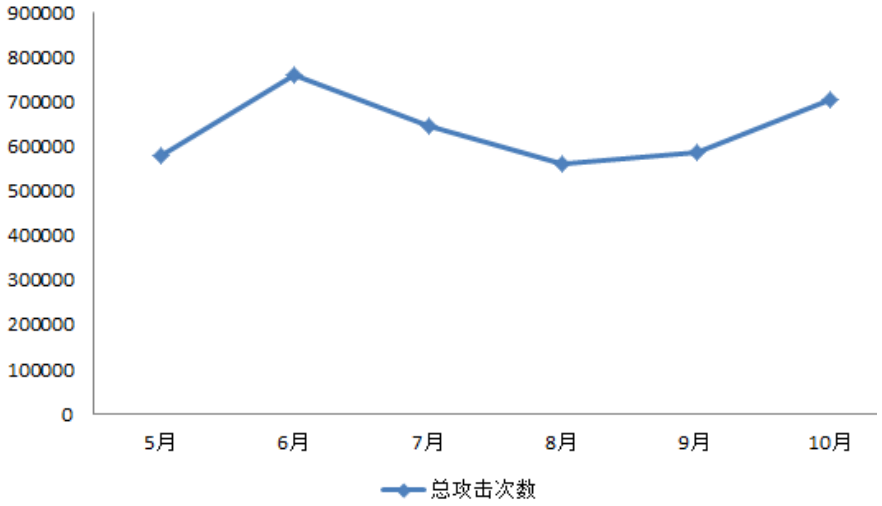
SYN Flood | TCP/UDP Flood | DNS Flood

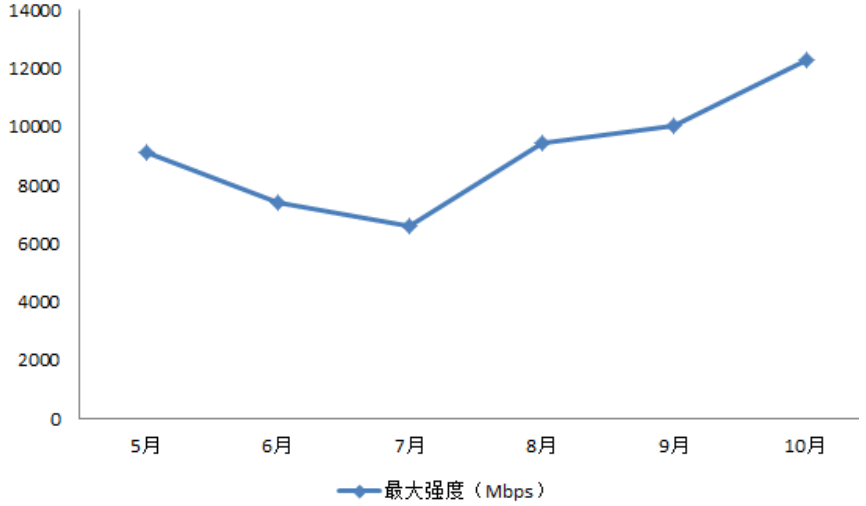
被攻击服务器	归属	类型	起始时间	终止时间
202.119.25.72	东南大学	21	2015-04-15 06:00:00	未终止
101.4.138.94	CERNET保留...	51	2015-04-15 07:40:00	未终止
121.195.187.68	北京世纪互联...	52	2015-04-15 08:35:00	未终止
222.199.191.49	北京百度网讯...	52	2015-04-15 09:40:00	未终止
74.125.136.138	美国	53	2015-04-15 10:23:53	未终止
74.125.136.139	美国	53	2015-04-15 10:25:56	未终止

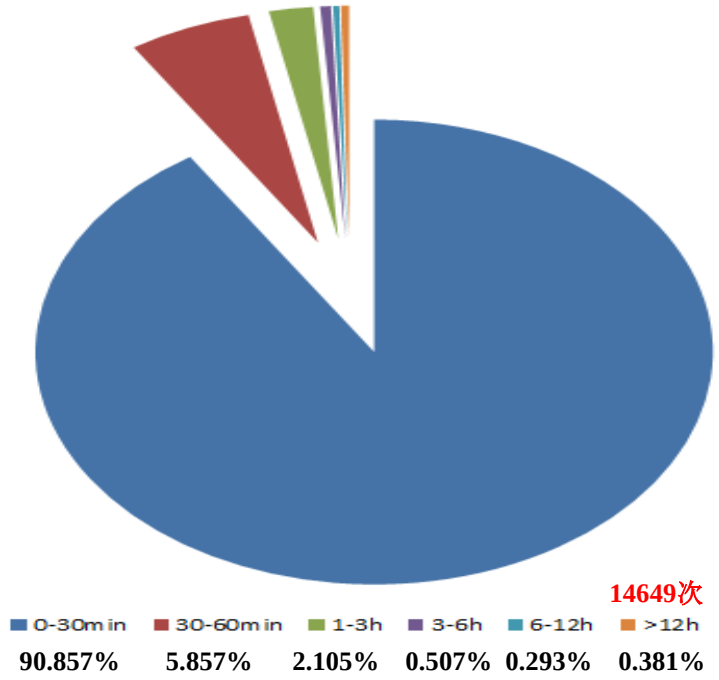
最近网内被攻击服务器 More...

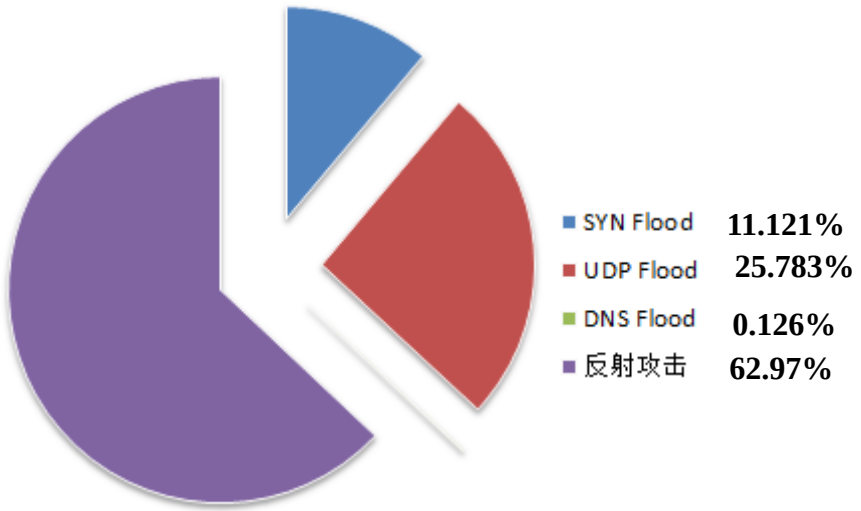
IP	归属	被攻击次数	最大强度(pps)	末次检出时间
202.119.25.72	东南大学	256	10263	2015-04-15 11:14:59
202.119.25.228	东南大学	185	8854	2015-04-15 11:09:59

NBOS对DDoS攻击的检测









检测到的最大强度攻击SYN-Flooding

2015年内被攻击服务器为42.247.11.5—42.247.11.5的记录

点击"最大IP数"列链接可见参与攻击的IP

点击显示四类极值记录

序号	被攻击服务器	归属	类型	起始时间	结束时间	持续时间(s)	活跃时间粒度数	pps	最大pps	Kbps	最大Kbps	平均报文长度(B)	平均IP数	最大IP数
1	47.11.5	浙江 学院	21	2015-10-03 14:00:01	2015-10-03 17:06:19	11178	62	975,660	1,949,256	6,201,262	12,575,042	813	578	725
2	47.11.5	浙江 学院	21	2015-09-19 16:25:01	2015-09-19 22:43:17	22696	148	496,950	2,728,680	1,965,677	10,302,185	506	61,974	179,501
3	47.11.5	浙江 学院	21	2015-06-23 15:30:00	2015-06-23 15:34:59	299	1	1,087	1,087	602	602	70	1,128	1,128

XXX.XXX.73.100

- 内部视频监控设备
- 海康威视高危漏洞事件

多种僵尸网络控制

- **85.118.XXX.XXX**

```
# /bin/busybox echo -ne \\x41\\x00\\xc0\\x1c\\x41\\x00\\x5c\\x00\\x00\\x00\\xa8\\x00\
\x00\\x00\\x06\\x00\\x00\\x00\\x00\\x00\\x01\\x00\\x51\\xe5\\x74\\x64\\x00\\x00\\x00\
\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\
\x06\\x00\\x00\\x00\\x04\\x00\\x00\\x00\\xc6\\x2f\\xe6\\x2f\\x22\\x4f\\xf3\\x6e\\x00\
\xa0\\x09\\x00\\x01\\xd1\\x02\\xc7\\x23\\x01\\x2a\\x40\\x98\\x00\\x00\\x00\\x01\\xd1\
\x02\\xc7\\x23\\x01\\x2a\\x40\\xcc\\x17\\x00\\x00\\xe3\\x6f\\x26\\x4f >> /var/mvXUDI
&& /bin/busybox WOPBOT
```

- 37.200.XXX.XXX

```
0000  45 08 00 55 24 09 40 00  2b 06 5d 74 25 dc 24 16   E..U$.@. +.]t%.$.
0010  3a c8 49 64 00 3d 96 25  47 9b 25 d4 9c f9 3b 2c   :.Id.=.% G.%...;,
0020  80 18 00 72 04 10 00 00  01 01 08 0a 17 04 11 b9        r
0030  1b a6 85 35 21 2a 20 53  59 4e 20 32 30 35 2e 31    ...5!* S YN 205.1
0040  34 37 2e 38 38 2e 35 36  20 34 34 33 20 33 30 30   47.88.56  443 300
0050  20 30 20 31 30                                      0 10
```

攻击目标与方式

DDoS攻击行为

- 2015年3月—今
- 2042次DDoS攻击
- SYNFLOOD攻击

序号	被攻击服务器	归属	类型	起始时间	结束时间	持续时间(s)	活跃时间粒度数	pps	最大pps	Kbps	最大Kbps	平均报文长度(B)
1	31.220.13.80	德国	53	2015-11-10 01:05:17	2015-11-10 01:06:17	60	1	7,271	7,271	3,749	3,749	65
2	31.220.13.80	德国	53	2015-11-09 23:55:56	2015-11-09 23:56:56	60	1	7,160	7,160	3,692	3,692	66
3	31.220.13.51	德国	53	2015-11-09 22:25:21	2015-11-09 22:30:02	281	2	1,350	1,362	695	702	65
4	31.220.13.151	德国	53	2015-11-09 22:25:21	2015-11-09 22:30:02	281	2	1,274	1,352	656	697	65
5	31.220.13.51	德国	53	2015-11-09 21:42:17	2015-11-09 21:43:17	60	1	1,132	1,132	583	583	65
6	31.220.13.151	德国	53	2015-11-09 21:42:17	2015-11-09 21:43:17	60	1	1,314	1,314	677	677	65
7	205.147.88.56	美国	51	2015-11-09 21:15:09	2015-11-09 21:19:59	290	1	21,106	21,106	11,381	11,381	69
8	31.220.13.191	德国	53	2015-11-09 11:50:19	2015-11-09 11:52:19	120	1	630	630	6,729	6,729	1367
9	31.220.13.191	德国	53	2015-11-09 09:46:09	2015-11-09 09:48:09	120	1	610	610	6,520	6,520	1368
10	31.220.13.191	德国	53	2015-11-09 08:06:12	2015-11-09 08:08:12	120	1	725	725	7,740	7,740	1366

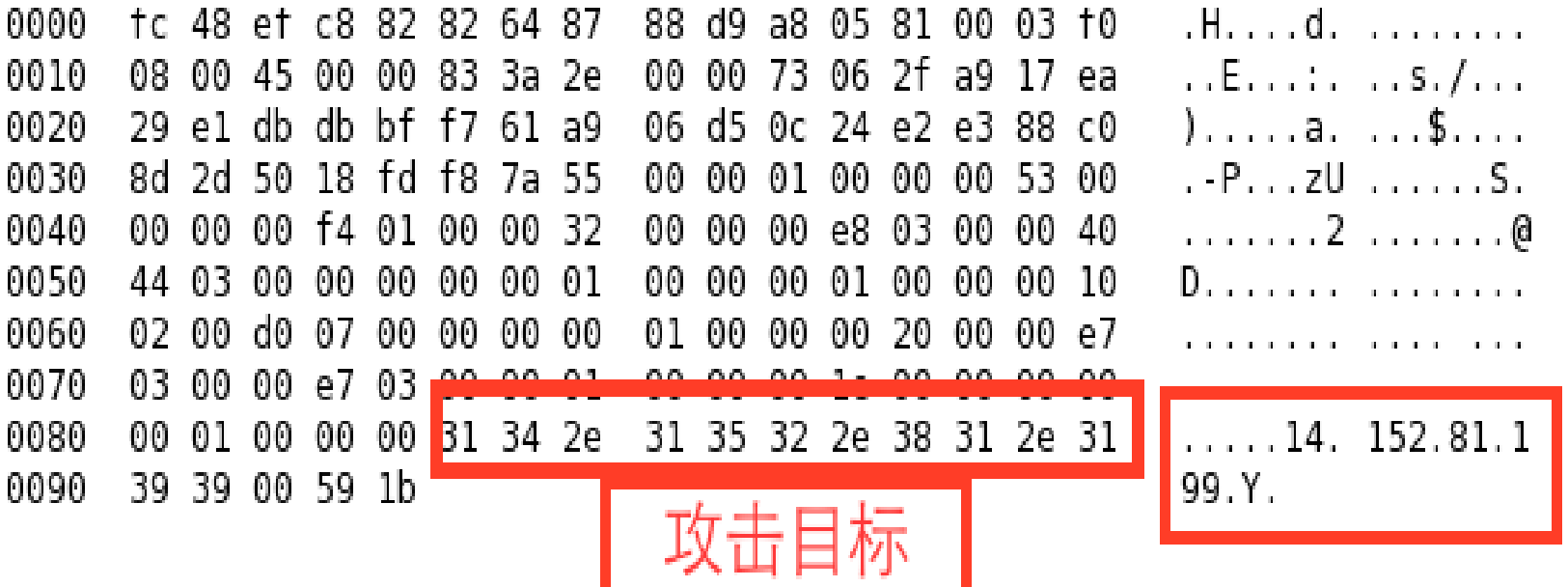
XXX.XXX.191.247

- 中国知网镜像服务器
- 教学资源参考数据库
- 装有瑞星杀毒系统

书名	领导学：理论、实践与方法	作者	王乐夫编著		
出版社	中山大学出版社	出版时间	1998年08月第1版	出版地	
ISBN	7-306-01454-4	页数	372		
索书号	C933	关键词	领导学-概论		
文摘					
适用课程	领导学(通识选修课)				
馆藏信息					
电子书	没有权限				
推荐人	管理员				

多个僵尸网络控制服务器

- **133.130.XXX.XXX**
- **202.102.XXX.XXX**
- **23.234.XXX.XXXX**
- 相同控制协议



活跃的DDoS攻击行为

- 2015.1 ～ 今
- 28000余起攻击
- SYNFLOOD

序号	被攻击服务器	归属	类型	起始时间	结束时间	pps	最大pps	Kbps	最大Kbps
1	106.122.251.123	电信	53	2015-11-14 22:06:53	2015-11-14 22:14:33	695	843	4,401	5,388
2	23.234.43.18	美国	51	2015-11-14 21:15:00	2015-11-14 21:19:59	587	587	3,495	3,495
3	106.122.251.123	电信	53	2015-11-14 21:05:00	2015-11-14 21:09:59	901	901	5,801	5,801
4	106.122.251.123	电信	51	2015-11-14 20:50:00	2015-11-14 21:04:59	964	1,054	6,250	6,962
5	59.36.97.139	电信	53	2015-11-14 19:05:00	2015-11-14 20:44:56	950	1,059	6,187	6,927
6	59.36.97.131	电信	53	2015-11-14 17:35:45	2015-11-14 18:24:54	1,403	1,608	10,485	12,015
7	59.36.97.204	电信	53	2015-11-14 17:16:34	2015-11-14 18:19:51	1,804	1,828	13,480	13,653
8	59.36.97.79	电信	51	2015-11-14 17:30:20	2015-11-14 18:19:46	1,622	1,695	12,123	12,653

CERNET全网DNS服务器数量统计

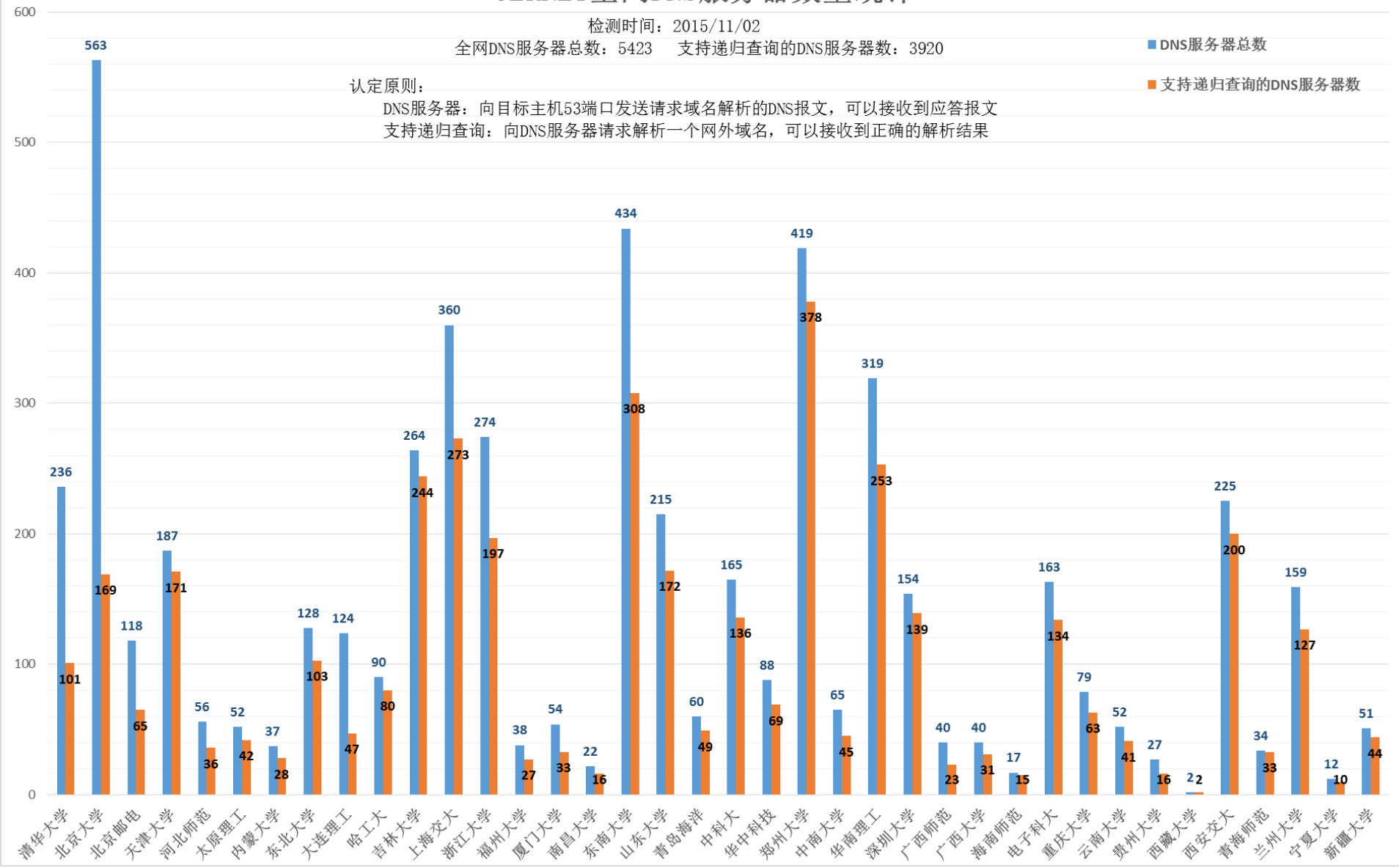
检测时间：2015/11/02

全网DNS服务器总数：5423　支持递归查询的DNS服务器数：3920

认定原则：

DNS服务器：向目标主机53端口发送请求域名解析的DNS报文，可以接收到应答报文

支持递归查询：向DNS服务器请求解析一个网外域名，可以接收到正确的解析结果



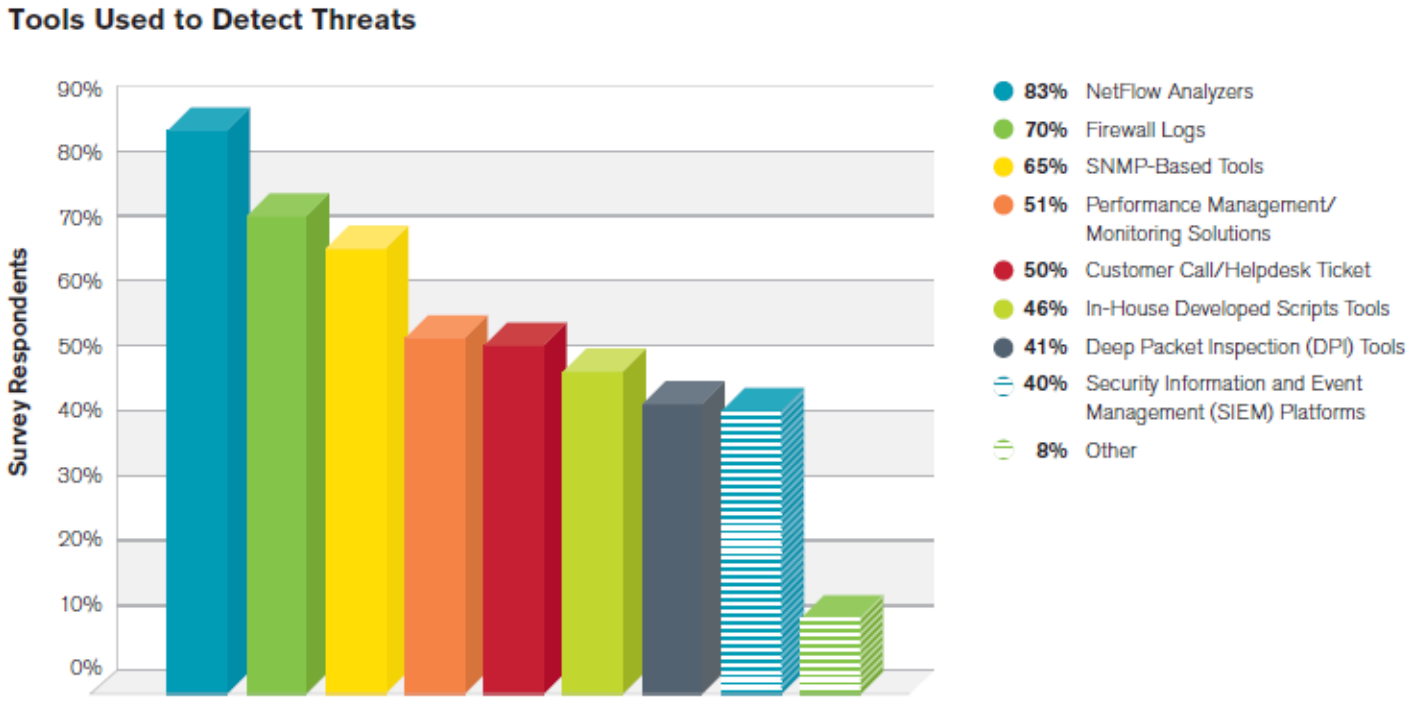
DDoS的防御架构

- 宿端防御机制
  - 在被攻击的宿点网络边界部署检测与防御系统，保护宿点服务的可用性。目标明确但效果可能不好，因为无法抑制源点。
- 源端防御机制
  - 在攻击源点的网络边界部署检测与阻截系统，拦截或限制攻击流量。可使攻击抑制效果最大化，但源点难以发现且缺乏利益驱动力。
- 主干网防御机制
  - 在互联网主干网中部署检测与阻截系统，拦截或限制攻击流量。检测难度介于宿端防御机制和源端防御机制之间，防御效果也介于两者之间。需要协同机制支持以达到理想的防御效果。由于作为ISP有服务质量保证的责任，因此对攻击防御有一定的利益驱动力。

DDoS的检测方法

- 基于统计方法
  - 针对Flooding类型的攻击，基于流量的统计特征来进行异常检测，重点是一些典型报文（例如TCP的SYN报文）的统计特征。这类方法的部署没有限制，在源端、主干网和宿端均可进行流量的异常检测。
- 软计算方法
  - 对不精确性和不确定性有一定容忍程度的异常检测方法，包括神经网络方法、遗传算法等等。这类法较多是用在宿端或主干网，针对放大类攻击进行流量的异常检测。
- 基于知识的检测方法
  - 针对基于协议及其实现的漏洞类型的攻击，基于预定义的攻击特征或模板进行检测，多部署在宿端或主干网中。

Arbor的调查结果-检测



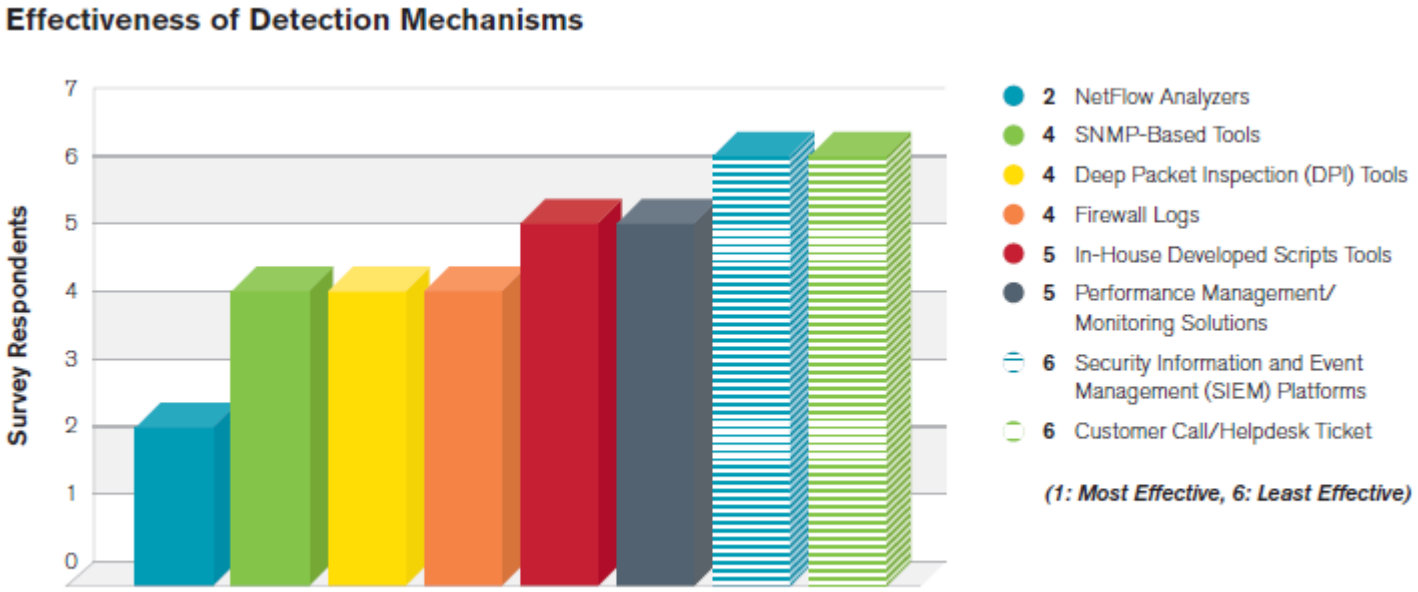


Figure 31 Source: Arbor Networks, Inc.

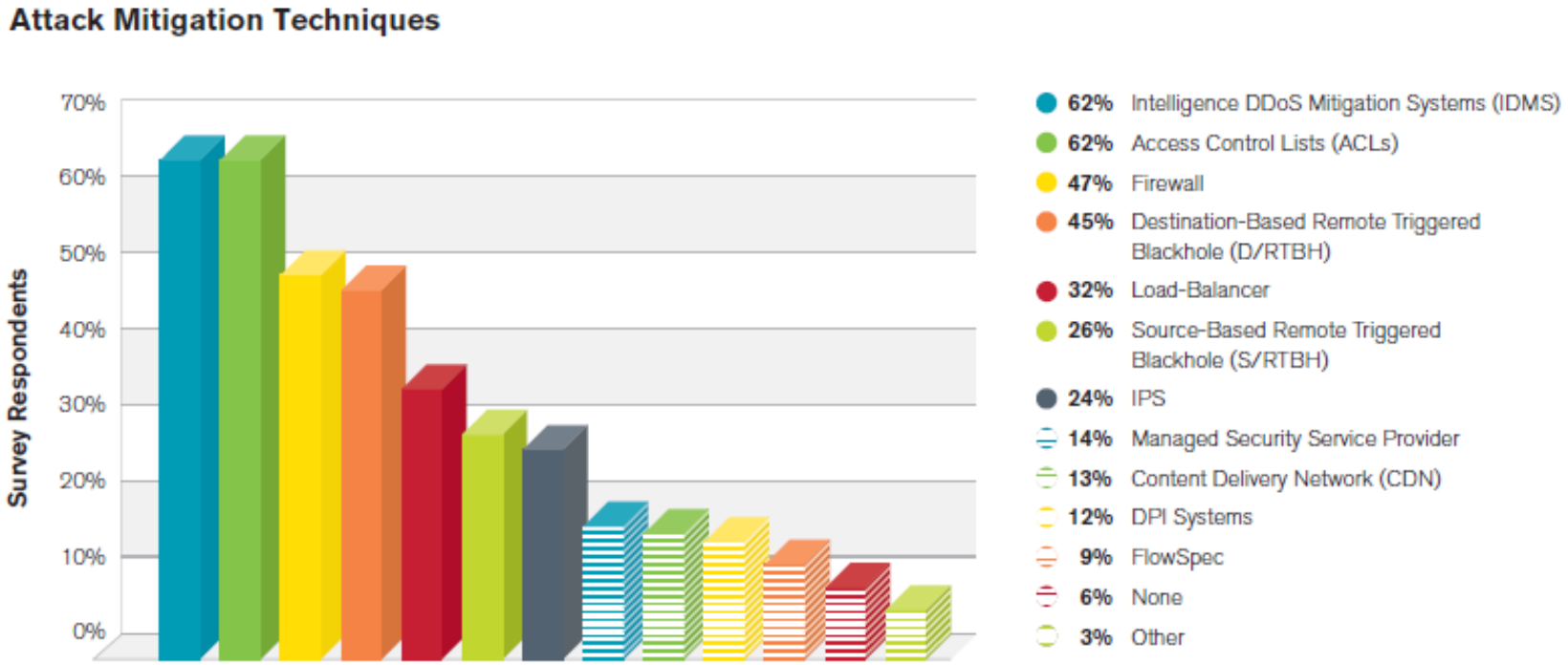
DDoS防御面临的挑战

- 随路检测方式的有效性：检测系统同时也受到攻击而无法正常工作；
- 响应的有效性：攻击检测的及时性，自适应的检测与响应联动机制，广泛的攻击抑制协同机制；
- 流量相似性的干扰：低速DDoS与正常流量相似，一般DDoS与突发流量相似，相似性导致检测精度过低；
- 检测系统对新的未知类型攻击的适应性：检测系统如何进化；
- 检测与防御系统的可部署性：对现有网络及其设备不产生负面影响；
- 检测与防御系统的性能要求：能够适应网络流量的增长现状和设备性能约束；
- 伪造源地址的攻击源追踪：需要协同机制的支持。

学术界的思路

- ***FireCol* relies on a distributed architecture composed of multiple IPSs forming overlay networks of protection rings around subscribed customers. Participating IPSs along the path to a subscribed customer collaborate (vertical communication) by computing and exchanging *belief* scores on potential attacks.**
- 协同防御的要点在于在攻击强度增强到单一防御系统不能处理之前就开始对其进行阻断，这要求在主干网中离被攻击对象尽可能远的地方就开始对攻击进行逐步地和协同地检测与拦截，以期同时解决攻击的大规模和源冒充问题。

FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks
Jérôme François, et.al.，IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 6, pp1828-1841, DECEMBER 2012



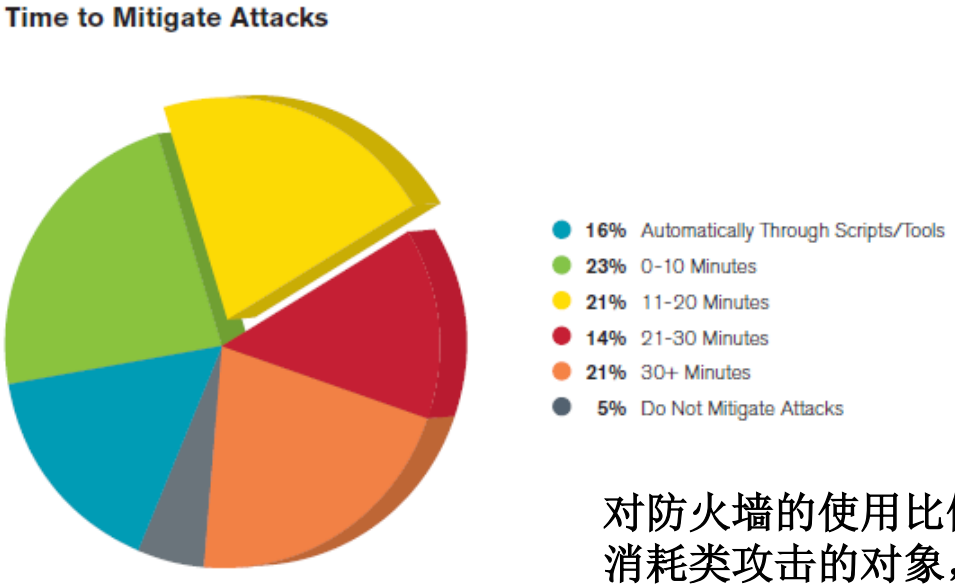


Figure 34 Source: Arbor Networks, Inc.

Arbor的调查结果-攻击阻断

对防火墙的使用比例在下降，因为它会成为状态消耗类攻击的对象，从而成为瓶颈，因此更多的用户选择使用智能阻断系统，例如黑洞。

基本防御机制

- 洗流　　In-line方法
  - ACL：粗粒度过滤
  - IPS：细粒度过滤

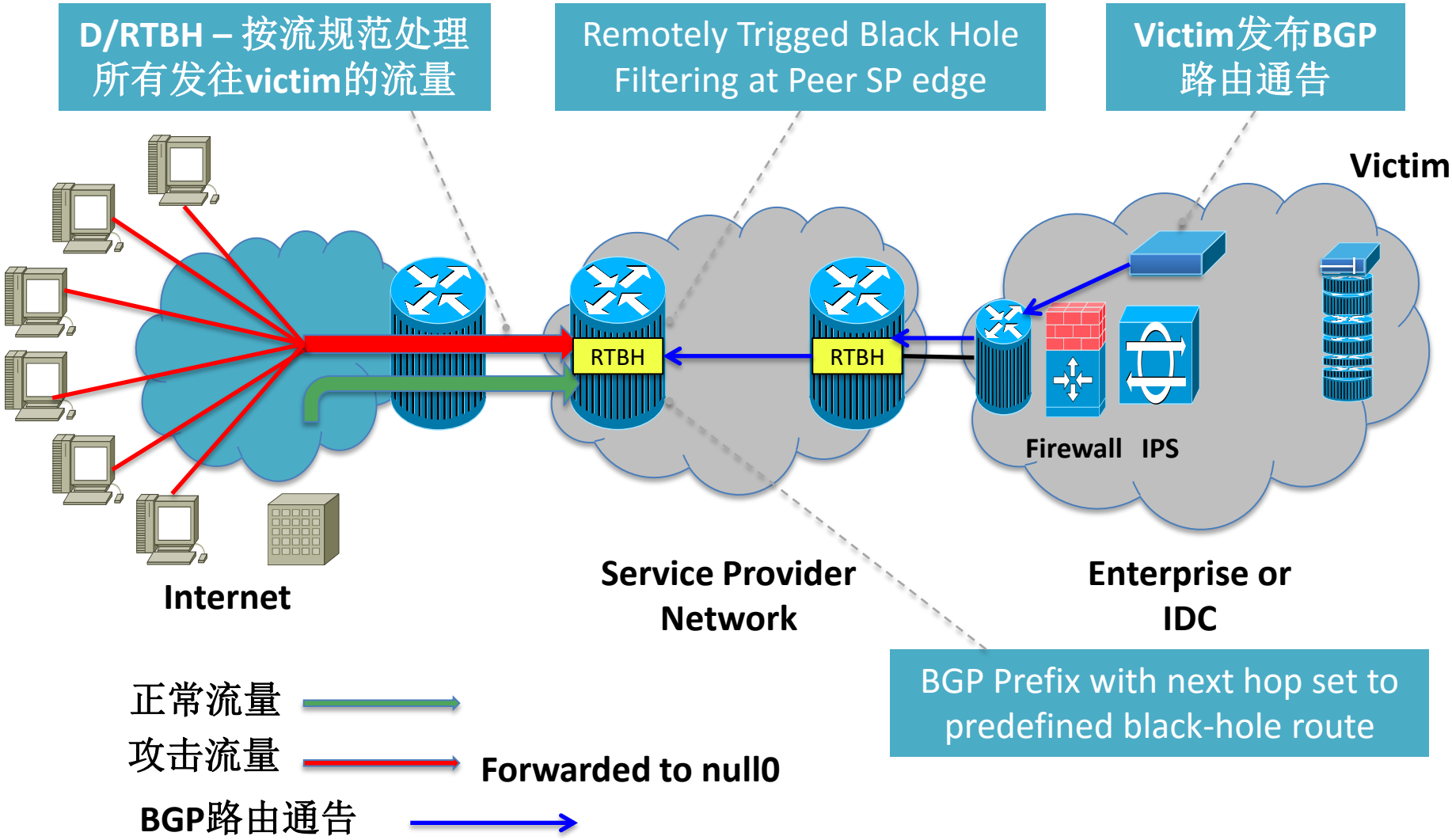
- 引流
  - Remote Triggered Black Hole (RTBH)
  - 可以基于宿地址或源地址

BGP Flowspec

- 可以使用的过滤测度
  - 源/宿地址前缀
  - IP报头的Protocol字段
  - 源/宿端口
  - ICMP的type和code字段
  - TCP的Flag
  - 报文长度
  - DSCP字段
  - Fragment字段
- 使用Extended Communities定义过滤动作
  - 0x8006：traffic-rate (rate 0表示丢弃该流所有报文)
  - 0x8007：traffic-action
  - 0x8008：redirect to VRF
  - 0x8009：traffic-marking

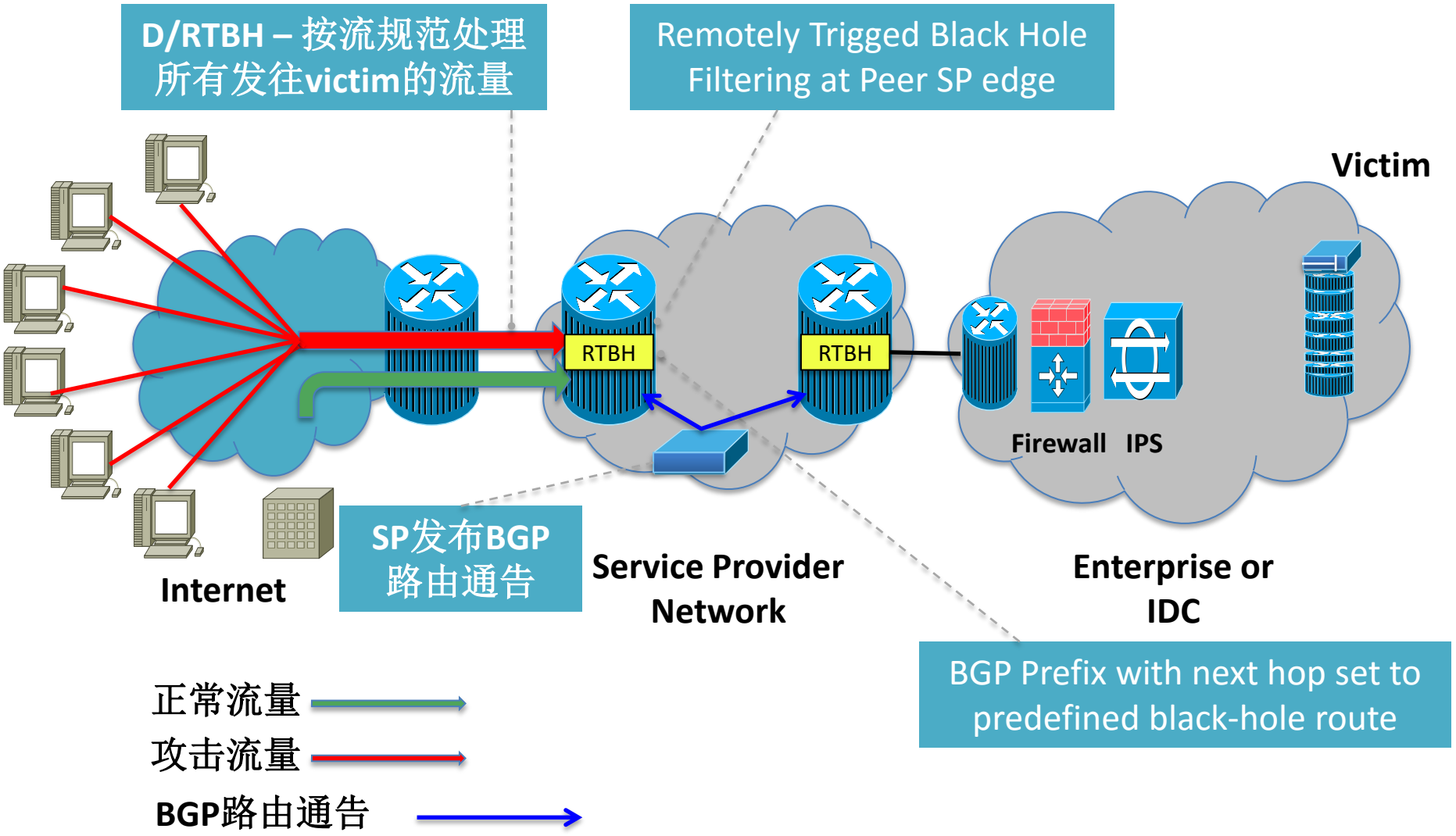
RFC 5635 - Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)
RFC 5575 - Dissemination of Flow Specification Rules
RFC 7674 - Clarification of the Flowspec Redirect Extended Community

Inter-domain Flowspec injection



RFC 5635 - Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)
RFC 5575 - Dissemination of Flow Specification Rules
RFC 7674 - Clarification of the Flowspec Redirect Extended Community

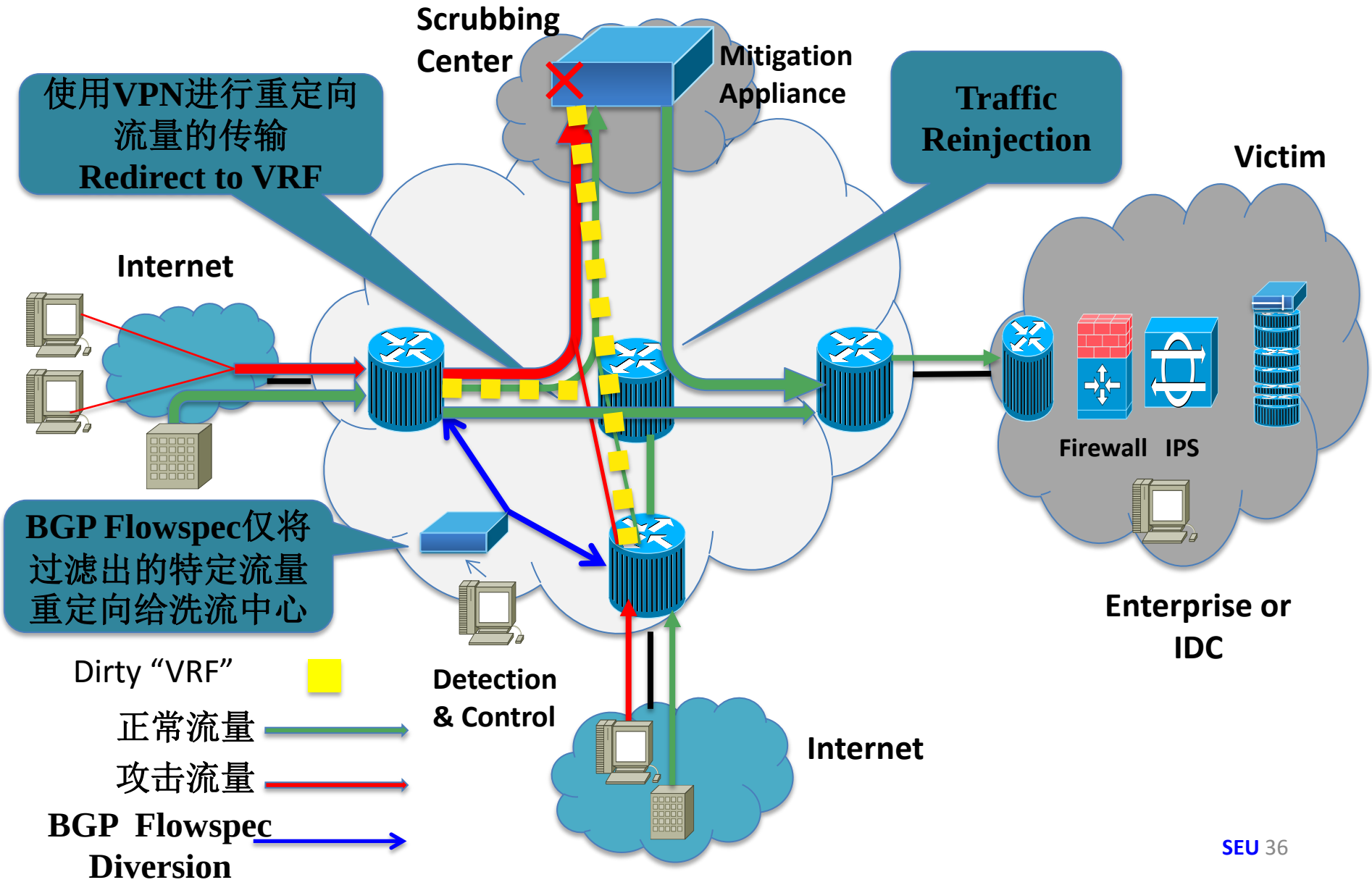
Intra-domain Flowspec injection



Intelligent DDoS Mitigation System

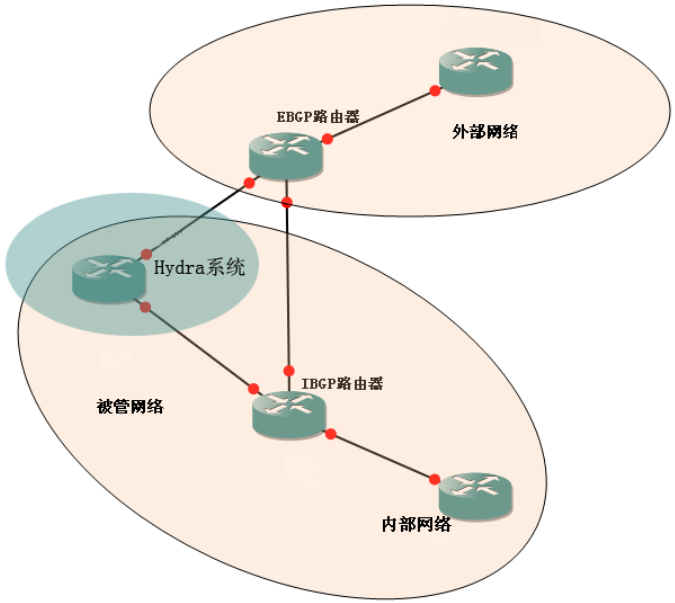
- 手术式阻断 (Surgical Mitigation)
  - 基于DPI技术的洗流技术，从流量中将攻击流剔除；
  - 通常是网络基础设施中的一个共享资源 (系统)；
  - 攻击流量需要在正常路由表 (GRT)中重定向以通过这个系统 (Traffic Diversion or Offramping)，按规则过滤后再 (隧道或VPN) 转发到实际的宿端 (Traffic Reinjection or Onramping)；

DDoS Mitigation Appliance – "Surgical Diversion" Using BGP Flowspec "Redirect to VRF" Action

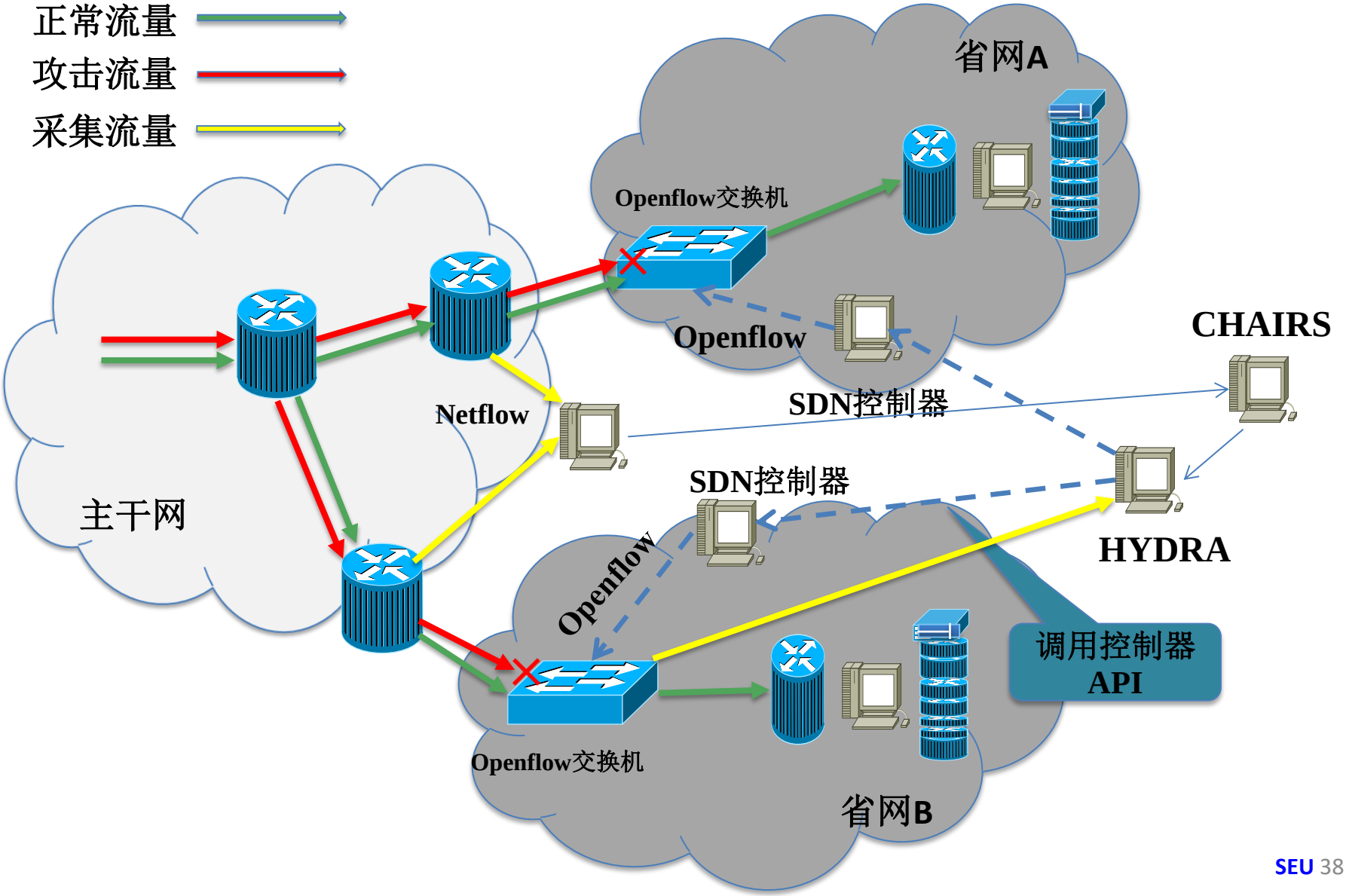


Hydra2.0系统

- **HYDRA1.0 (混合检测响应系统，HYbrid Detection Response Agent)系统是在国家科技支撑计划课题“新一代可信任互联网安全和网络服务”和211二期CERNET建设项目支持研制的网络安全事件应急响应系统。**
  - **Traffic diversion & Scrubbing**
  - **手工配置**
  - **GE环境**
- **Hydra2.0系统**
  - **基于SDN技术**
  - **Scrubbing & Intrusion detection & Sniffing**



Hydra2.0系统架构



Hydra2.0测试


混合检测响应系统
HYbrid Detection Response Agent
首页
控制器
交换机
管理中心
管理功能列表
执行节点
交换机及控制器
用户管理
交换机状态
作业状态
交换机配置
历史日志
控制器状态
历史规则
控制器配置

Hydra2.0测试

混合检测响应系统

HYbrid Detection Response Agent

首页　作业　规则　个人中心

作业状态如下：

序号	规则详情	当前状态	失效条件	操作
1	IP协议：UDP 源宿地址段： 211.65.193.0/24 源宿端口：53 动作：采集	提交时间：2015-11-20 10:06:05 当前报文：2,150,865 当前流量：154,862,280 运行时间：365s	最大流量：1,000,000,000	停止 删除
2	IP协议：TCP 源宿地址段： 211.65.193.0/24 源宿端口：53 动作：采集	提交时间：2015-11-20 10:06:15 当前报文：15 当前流量：1920 运行时间：355s	最大报文：1,000	停止 删除
3	IP协议：ICMP 源宿地址段： 211.65.193.183/32 动作：阻断	提交时间：2015-11-20 10:06:33 当前报文：911,030 当前流量：89,280,940 运行时间：338s	结束时间：2015-11-20 12:00:00	停止 删除

Hydra2.0测试

混合检测响应系统

HYbrid Detection Response Agent

首页 作业 规则 个人中心

历史规则及最后状态

作业状态

序号	协议号	源IP及掩码	宿IP及掩码	源端口	宿端口	动作	报文数	字节数	存活时间	提交时间	失效时间	删除	激活
1	UDP	172.16.115.0/24				采集	118	12,758	20	2015-06-06 16:29:33	2015-06-06 16:29:55	删除	激活
2	UDP	172.16.115.0/24				阻断	4,345	521,763	554	2015-06-06 16:38:35	2015-06-06 20:37:23	删除	激活
3	TCP	172.16.113.0/24				采集	18,172	2,330,614	361	2015-06-06 16:40:50	2015-06-06 16:46:54	删除	激活
4	TCP	172.16.114.0/24				阻断	0	0	4	2015-06-06 16:42:24	2015-06-06 16:42:30	删除	激活
5	TCP	172.16.114.0/24				采集	15	900	288	2015-06-06 16:43:01	2015-06-06 20:37:23	删除	激活
6	ICMP	211.65.193.183/24				阻断	0	0	0	2015-11-18 22:01:08	2015-11-18 22:47:51	删除	激活
7	ICMP	211.65.193.183/24				阻断	0	0	0	2015-11-18 22:49:26	2015-11-18 22:58:29	删除	激活
8	ICMP	211.65.193.0/24				采集				2015-11-18 22:57:02	2015-11-18 22:58:29	删除	激活
9	ICMP	211.65.193.0/24				采集	0	0	0	2015-11-18 22:58:54	2015-11-18 23:03:06	删除	激活

小结

- DDoS攻击广泛存在并具有一定威胁
  - 在CERNET内的观测是每月数十万起
- 对DDoS攻击及其防御的研究是热点
  - RTBH是BCP
- DDoS攻击的遏制需要协同机制支持
  - 逐步地感知和阻截
- 主机安全管理仍然是重点问题
  - 僵尸主机
  - 网站漏洞
  - 管理意识和能力的提高

谢谢！