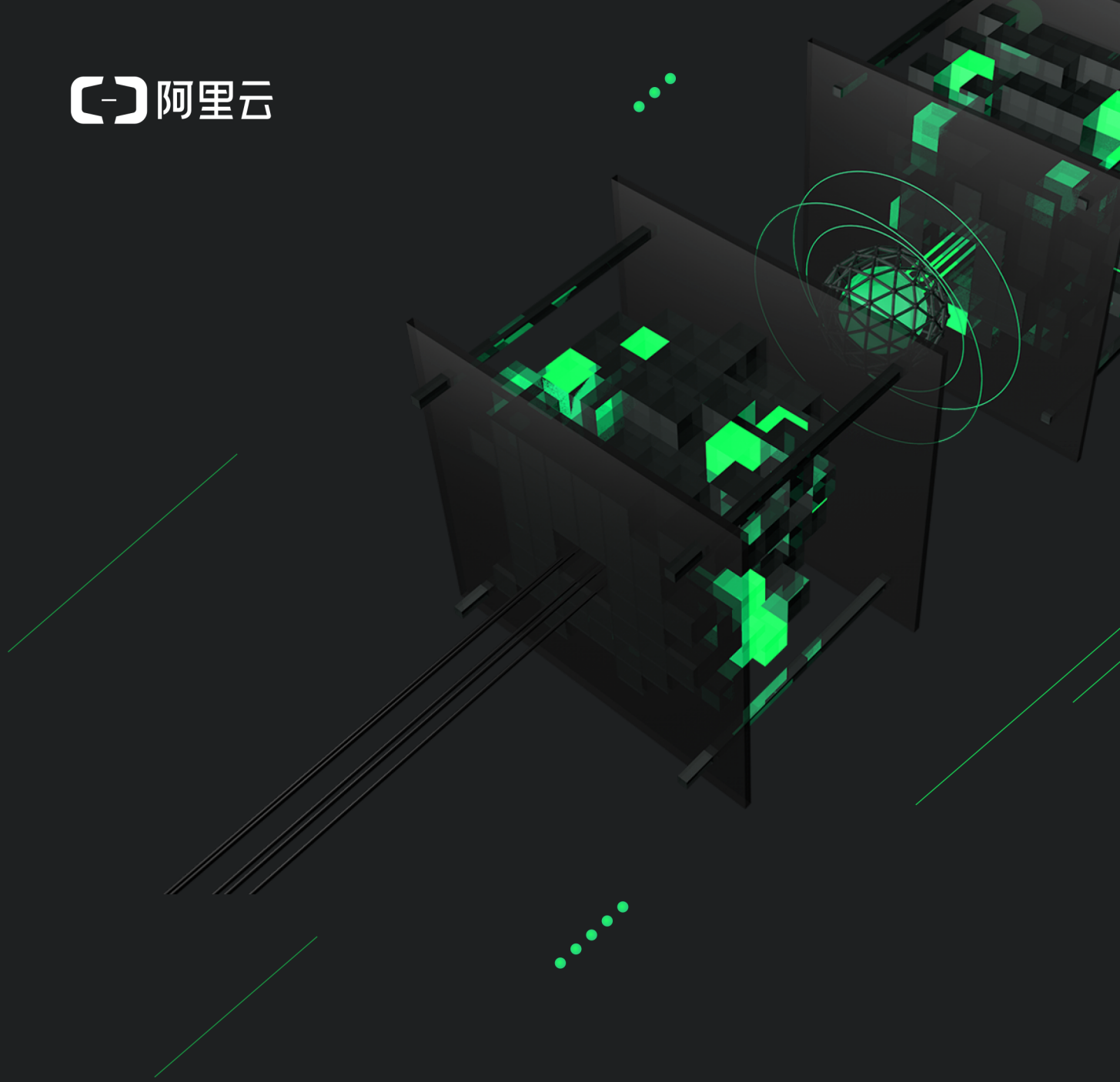
阿里云



2018年
DDoS攻击态势报告

阿里云安全团队

2019.03

2018年，阿里云安全团队监测到云上DDoS攻击发生近百万次，日均攻击2000余次。目前阿里云承载着中国40%网站，为全球上百万客户提供基础安全防御。可以说，阿里云上的攻防态势是整个中国攻防态势的缩影。阿里云安全团队基于2018.1.1-12.31阿里云上的DDoS攻击数据，从DDoS攻击事件、僵尸网络中控、DDoS肉鸡等多个维度做了统计分析，希望为政府和企业客户提供参考价值。

概述

经过有关部门以及企业的联合整治，相比2017年DDoS攻击次数降低了约22%。虽然DDoS攻击在数量上有减缓的态势，但经过数据分析发现，DDoS的攻击手法更加多样，针对同一用户DDoS攻击的平均次数有所增加。

2018年针对企业用户的DDoS攻击中，单一攻击流量的DDoS攻击比例减少10%，应用层的攻击比例增加了30%。更多的DDoS攻击使用混合流量，表明攻击者企图通过组合攻击的方式找到防护方的弱点，任意一种流量的漏过都可能导致防护层后面的服务瘫痪。同时，攻击者增加应用层的攻击流量，这要求应用层流量分析必须准确且自动化的产出清洗策略，这给流量清洗服务带来更大的挑战。DDoS攻击手法的变化，对流量清洗服务的准确性和自动化能力提出更高的要求，是企业和DDoS防护厂商需要提高注意的地方。

另外，2018年针对同一用户的DDoS攻击次数增加了21%，表明攻击者更有恒心达到其诉求，所以在遭到DDoS攻击时需要及时识别到风险并做好风险管理预案。抱有侥幸心理接受风险的做法可能意味着承受比以前更大的损失。

1. 攻击态势

1.1 攻击趋势

阿里云安全团队统计了2018年峰值流量超过50Gbps以上的DDoS事件分布，如图2-1所示；同时统计了2018年DDoS攻击月度峰值流量趋势，如图2-2所示。从图中可以看出，2018年DDoS峰值流量大于50Gbps事件有1.6万次，与2017年相比有大幅度降低。2018年，阿里云安全团队为某游戏客户成功抵抗了峰值流量超过1Tbps的DDoS攻击，DDoS攻击进入Tbps 时代。
由此不难看出，虽然DDoS大流量攻击数量有所下降，但攻击强度和目的性有所增强。

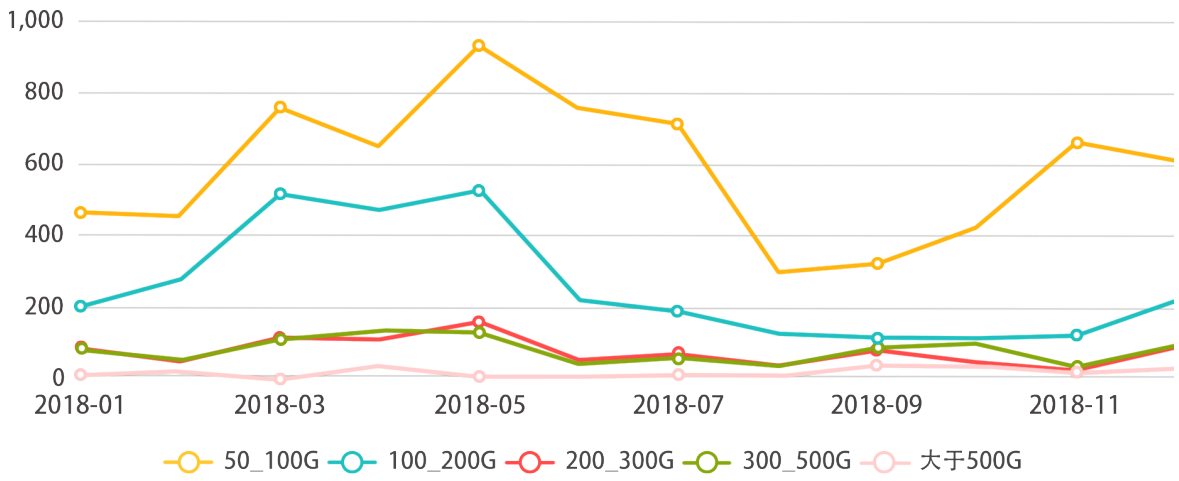


图1-1 2018年峰值流量大于50Gbps事件分布

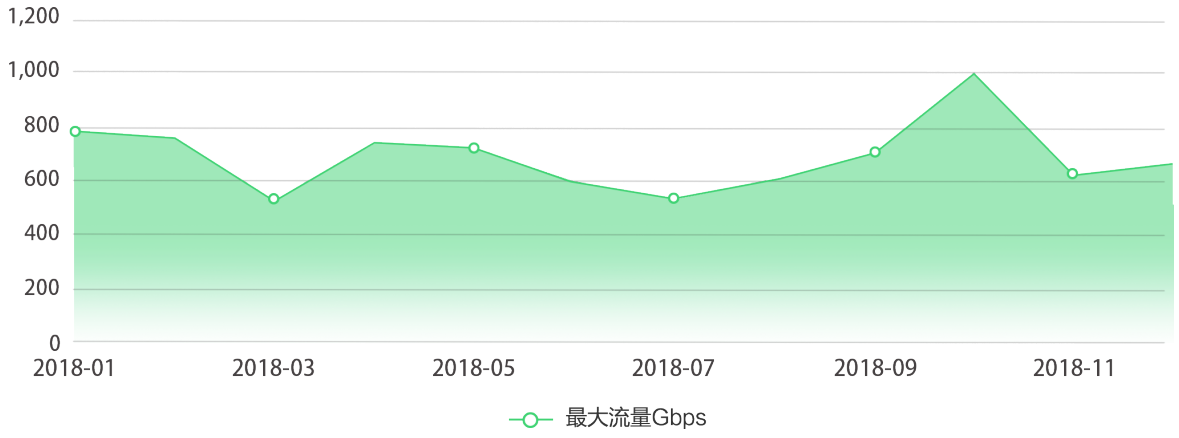
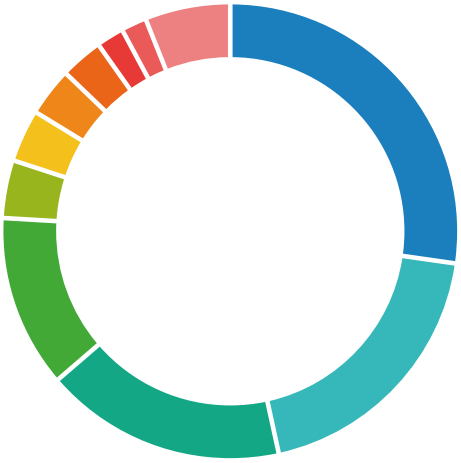


图1-2 2018年DDoS攻击峰值流量趋势

1.2 攻击行业分布

网站和游戏行业是主要的DDoS攻击目标，两者共占据DDoS攻击目标的46.85%。网站因为基数大占比最高，游戏由于对网络质量要求高,也容易成为被攻击的目标。另外统计还发现DDoS攻击更容易发生在16:00-20:00的时间段，游戏行业更容易在周一遭到攻击。

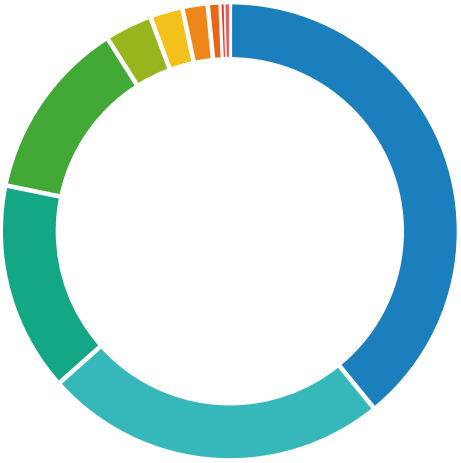


网站：27.26%　游戏：19.32%　互联网服务：17.11%
计算机软件和服务：12.24%　电子商务：4.1%　移动APP：3.72%
金融：3.43%　教育：3.03%　音视频：1.95%
通讯社交：1.8%　other：6.04%

图1-3 DDoS事件行业分布

1.3 攻击种类分布

当前存量反射源最多的攻击类型分别是SSDP、DNS、CLDAP、Memcached。UDP Flood仍然是最常见的攻击类型，但是由于UDP Flood 易清洗已经有下降的趋势。Memcached反射攻击因为放大倍数大，存量反射源多已经成常见的攻击手法。



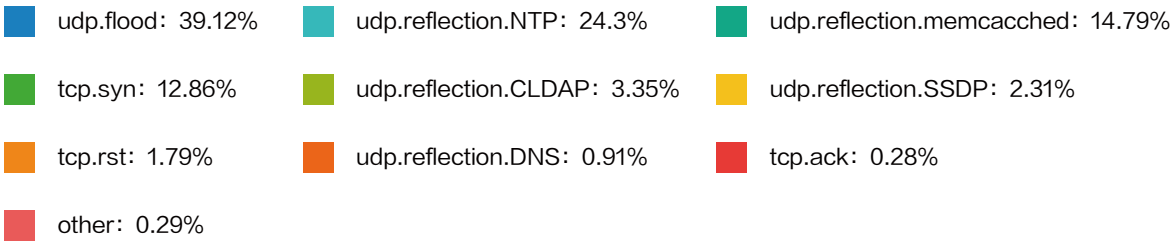


图1-4 2018 DDoS攻击种类分布

1.4 攻击目的端口分布

Web服务和游戏端口的DDoS攻击仍是主要的攻击目标，分别占比23%和13%，分布情况整体与行业DDoS攻击事件相符合。

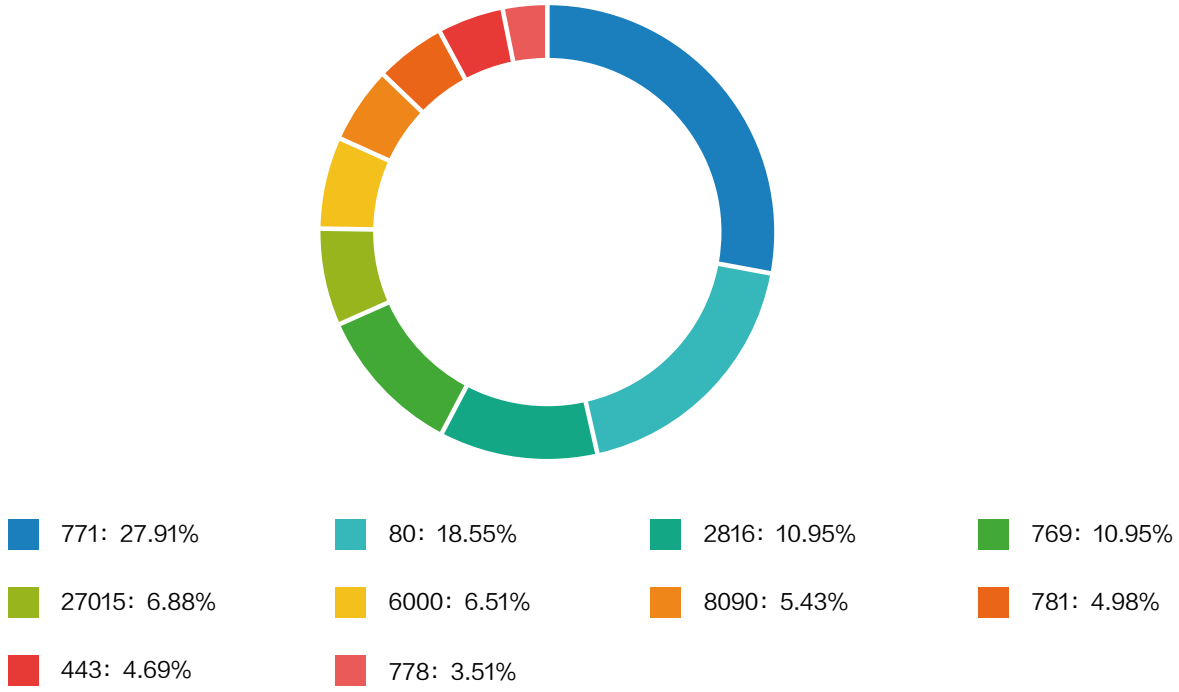


图1-5 DDoS攻击目的端口分布

1.5 核心观点

相比去年，2018年DDoS攻击的事件数趋于缓和，但DDoS攻击带来的挑战却越来越大。主要表现在以下几个方面：

1.TCP类型的攻击在DDoS攻击威胁中占据着更重要的比重。得益于运营商、云厂商、IDC等各方对于DDoS反射源的治理加强，UDP反射类型攻击在整个DDoS攻击中的占比有下降的趋势，而基于肉鸡的TCP类型的攻击方式则得到了加强。这种变化将使得攻防双方的对抗变得更为激烈。

2.应用层攻击对抗越来越激烈。应用层攻击变化越来越多，攻击者也通过变化攻击特征和手法，来绕过传统DDoS防御规则，因此若完全依靠于DDoS防御专家手工分析攻击报文来调整防御策略，那专家疲于救火，根本无法满足响应时间要求，导致用户业务恢复时间长。此时，智能防护能力显得愈发重要，能够基于用户业务历史情况产生符合用户业务的基线，同时智能判断攻击情况，根据攻击特征自动调整策略，确保快速防护，使用户业务得到秒级恢复，并确保不影响用户业务连续性。

3.游戏等行业依然是攻击发生最频繁的区域。利润丰厚、对网络质量要求高、同质竞争激烈是这些行业的特点。为了赢得更多的用户，赚取更多的利润，行业内部激烈的恶意竞争使得DDoS攻击长盛不衰。

4.攻击峰值已经以T为单位。随着新的DDoS攻击方式涌现，DDoS已经进入了T级峰值时代，并且在不断刷新记录。

5.DDoS攻击中，IoT设备的数量明显提升。随着物联网的普及，越来越多的智能硬件走进千家万户。但是不管是生产厂家，还是普通民众，信息安全意识都还相对薄弱。智能硬件的联网为黑客发起更大规模的攻击创造了绝佳机会。我们相信在未来比较长的一段时间内，这一趋势不会有明显的改变。

2. DDoS僵尸网络分析

2.1 木马家族分布

随着移动互联网的普及，在TOP10的木马家族中，Mirai、Dofloo和Gafgyt是针对IoT的木马病毒，已经占据DDoS木马的的44%。

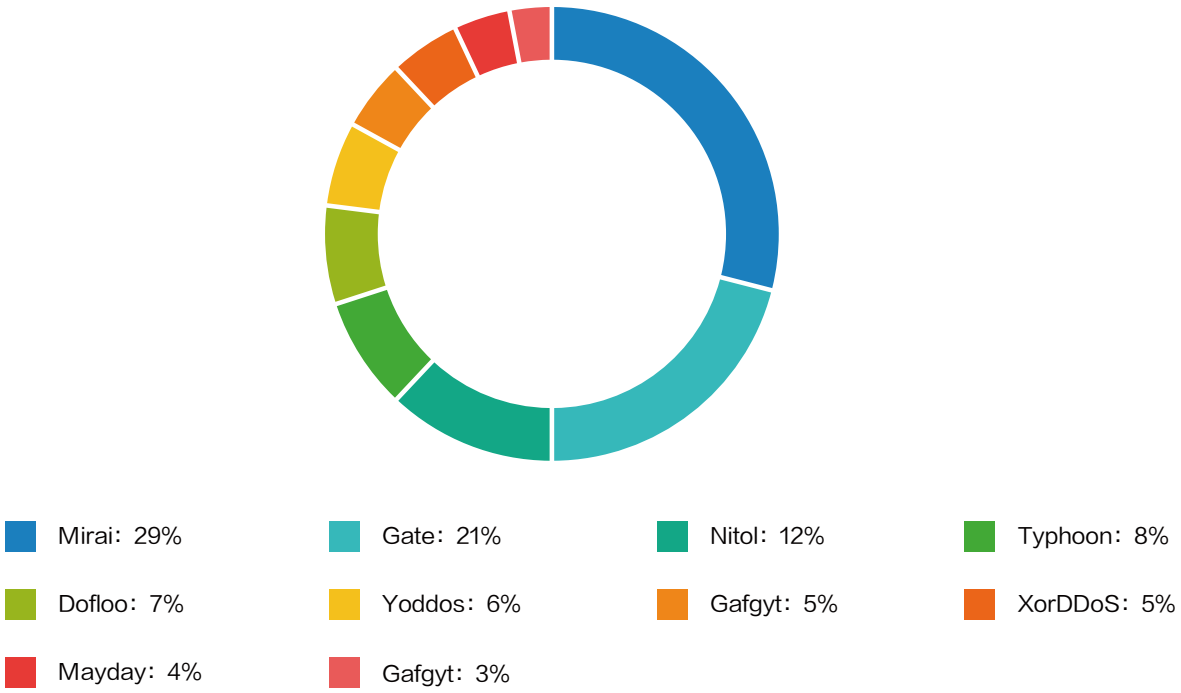


图2-1 DDoS木马家族分布

2.2 CnC地区分布

针对国内进行DDoS攻击的僵尸网络中，71%来自中国大陆，来自美国和香港地区的分别占13%和6%。

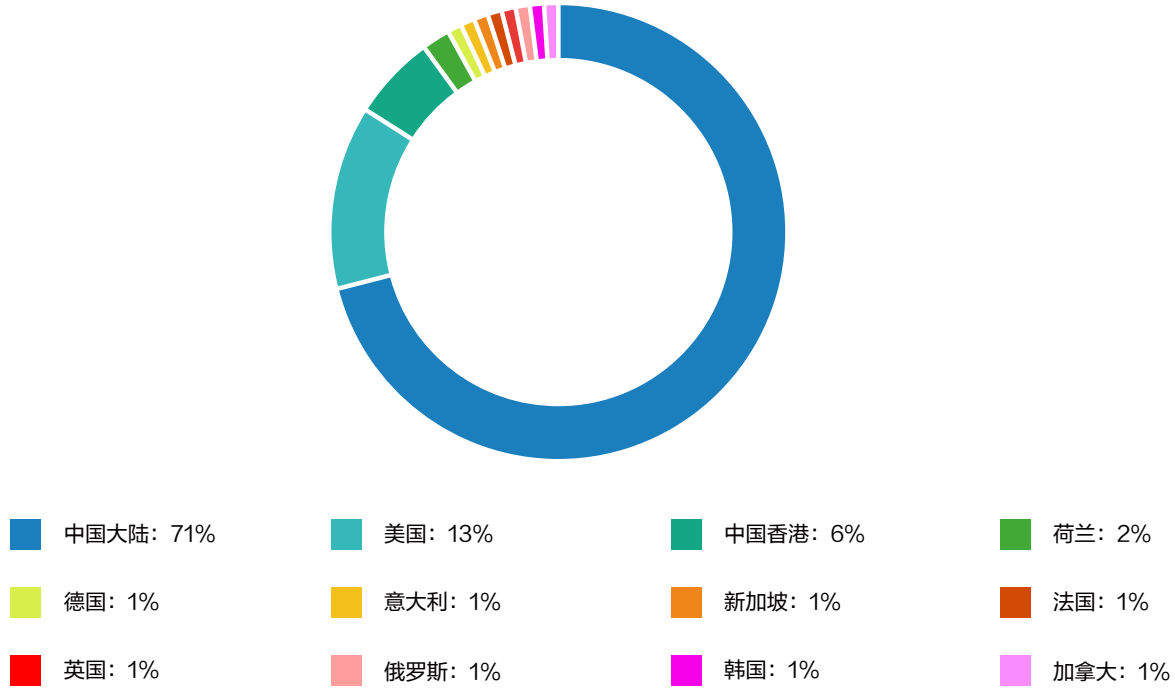


图2-2 CnC国家和地区分析

2.3 CnC存活时间分布

通过对CnC的存活时间进行分析发现，CnC的更新很频繁。63%的CnC存活时间不超过1周。

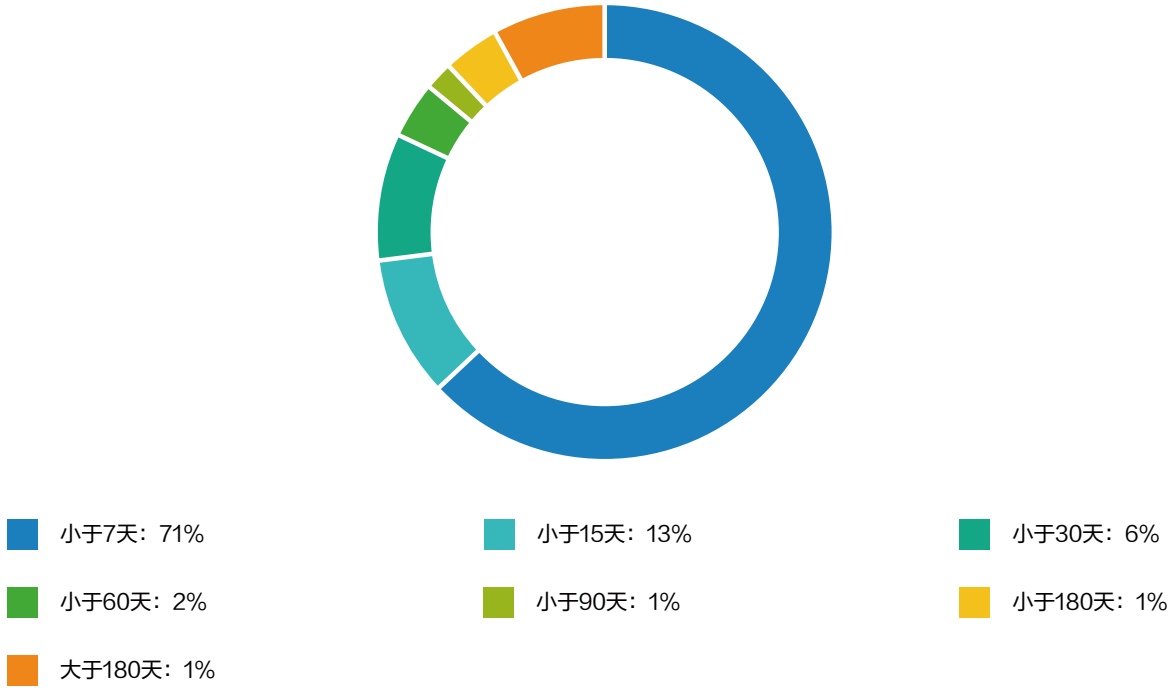


图2-3 CnC存活时长分布

3. DDoS肉鸡分析

3.1 UDP反射源国家分布

当前针对中国进行攻击的UDP反射源有50%来自中国大陆，俄罗斯和美国分别占15%和9%。主要因为这三个国家的互联网行业相对发达，能做UDP反射攻击的资源更多。

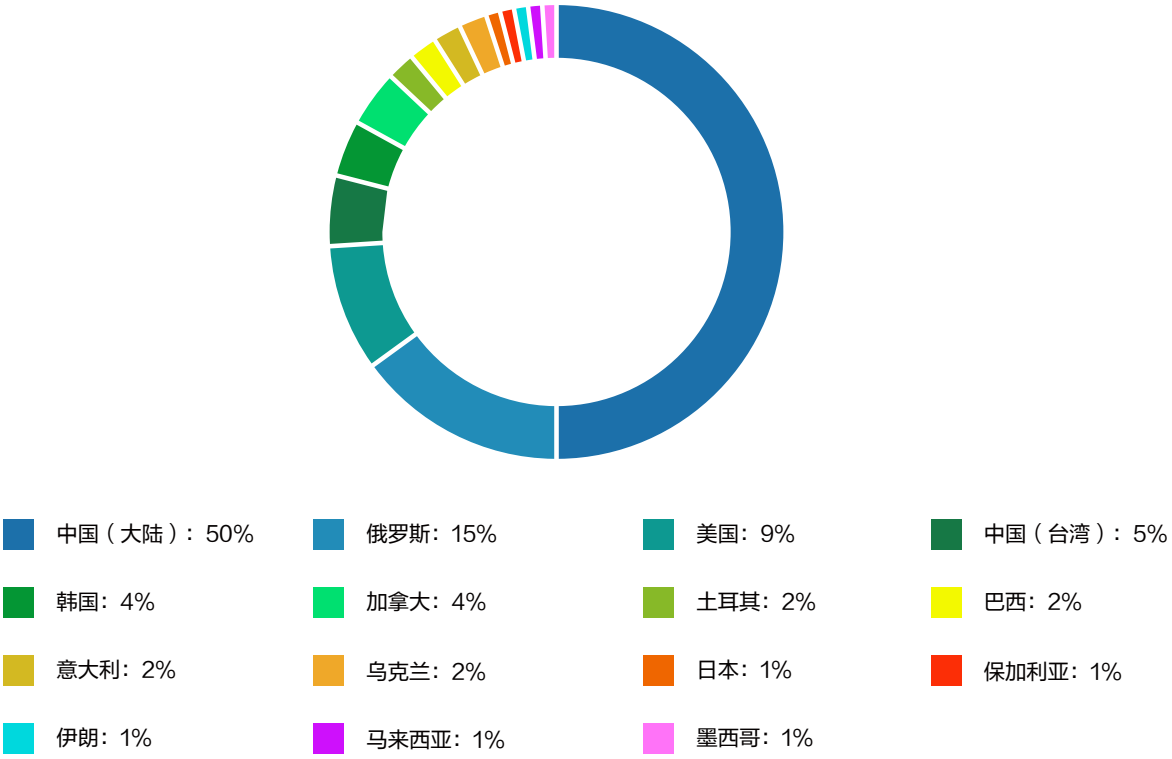


图3-1 UDP反射源国家及地区分布

3.2 肉鸡国家分布

在2018年对国内发起DDoS攻击的肉鸡IP中，62%来自中国大陆。2018年12月300G以上攻击事件中，43%都有一定比例海外攻击流量。阿里云安全团队建议当遭到大流量DDoS攻击时，可以结合攻击流量的运营商来源进行海外流量的封堵，以缓解大流量攻击。

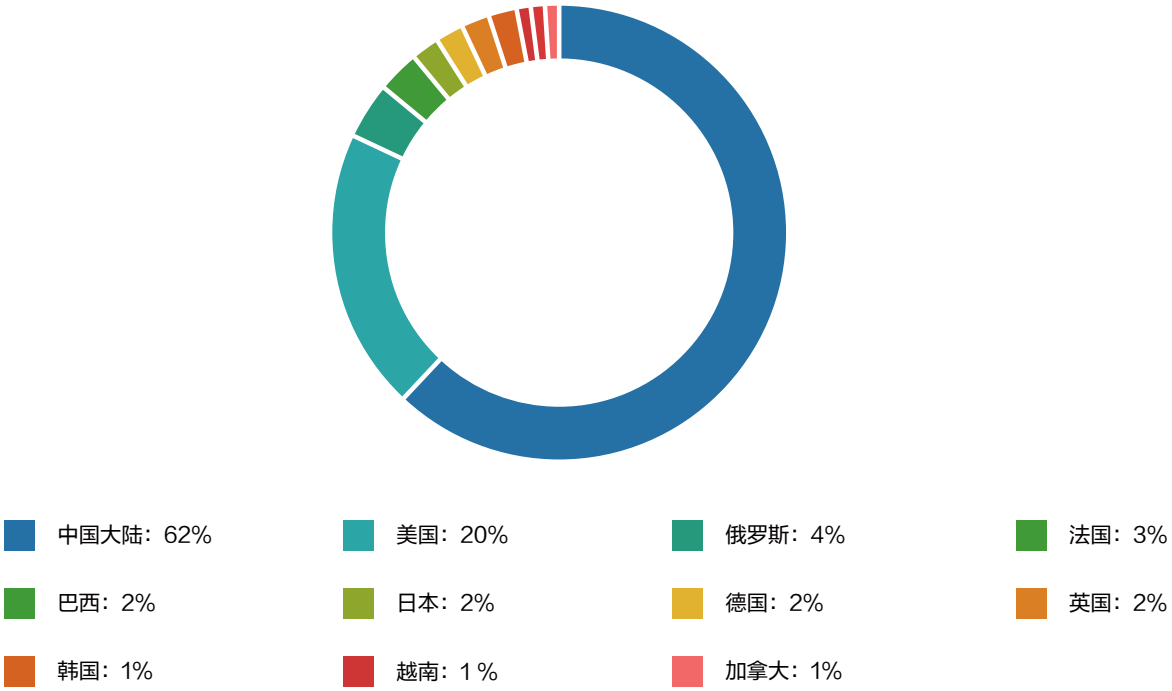


图3-2 肉鸡国家分布

3.3 肉鸡省份分布

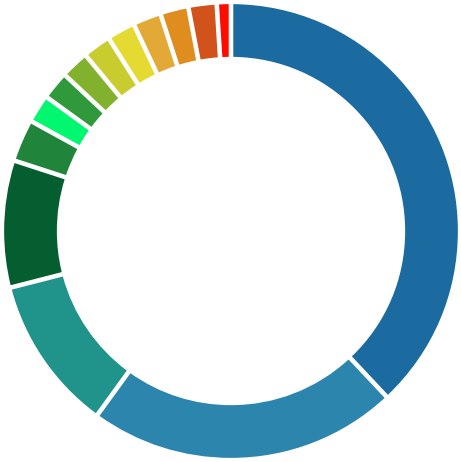
2018年共发现国内肉鸡IP 100万以上。由于互联网行业比较发达，上海和杭州占据国内肉鸡总量的41%。

上海市：29%　浙江省：12%　广东省：7%　辽宁省：6%
北京市：5%　江苏省：5%　山东省：4%　河北省：4%
四川省：3%　河南省：3%　福建省：2%　台湾省：2%
贵州省：2%　湖北省：2%　黑龙江省：2%　吉林省：2%
山西省：2%　云南省：2%　湖南省：2%　江西省：2%
其他：2%

图3-3 肉鸡省份分布

3.4 DDoS攻击运营商流量分布

2018年发生的DDoS攻击中有29%的流量来自海外，其中19%的攻击流量来源是美国。在国内的DDoS攻击流量中，中国电信是主要的DDoS攻击流量来源。



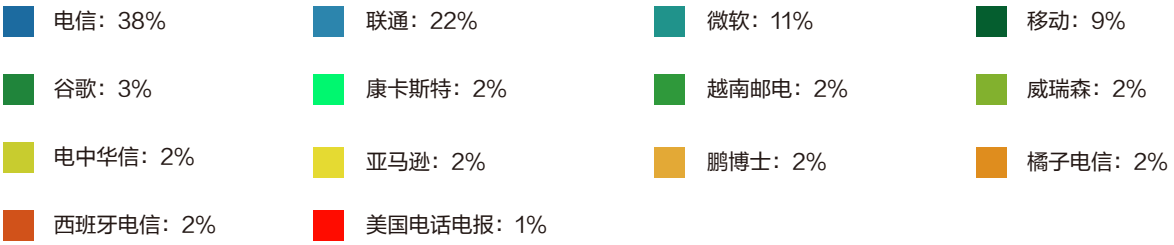


图3-4 DDoS 流量运营商分布

4. 典型案例

4.1 DDoS事件汇总

DDoS主要是针对互联网服务可用性的攻击，由于越来越多的企业开始基于互联网提供服务，因此DDoS攻击带来的影响也越来越大。2018年几乎每个月都有影响巨大的DDoS攻击事件发生。表4-1汇总了2018年影响较大的DDoS攻防事件：

201801	荷兰三大银行遭到DDoS攻击，业务集体瘫痪
201802	GitHub遭到DDoS攻击，峰值1.35Tbps
201803	Memcached 反射攻击POC公开
201804	欧洲最大DDoS服务商webstresser.org被关停
201805	美国监控到无线设备1.7Tbps DDoS 攻击
201806	加密邮件服务商ProtonMail因遭到DDoS攻击业务频繁掉线
201808	多家游戏公司遭到大规模DDoS扫射攻击
201810	阿里云主要节点全面上线IPv6 DDoS防护服务
201810	阿里云成功为某游戏客户抵抗峰值大于1Tbps的 DDoS攻击
201811	柬埔寨全国频繁断网，因主要网络服务提供商遭到大规模DDoS攻击
201812	匿名者宣布对全球银行发动DDoS攻击

表4-1 2018 DDoS大事件汇总

4.2 流量最大案例

2018年9月，阿里云云盾高防产品接入了一个游戏客户。业务上线后不久，该客户就频繁遭到DDoS攻击，平均每天要遭受两次10G左右的DDoS攻击，在阿里云DDoS高防的防护下，对业务并未产生影响。

10月13日，阿里云监测到该客户遭受的攻击峰值流量达到了430Gbps；3天后，攻击者调动了更多资源，希望一次性将业务置于死地；10月16日凌晨，该客户再次遭受DDoS攻击，流量峰值达到1.022Tbps，pps峰值则达到了6.9亿。收到攻击告警之后，阿里云安全团队检查攻击情况及客户业务状况，云盾高防运行平稳，攻击流量在可控范围内，攻击手法为大流量SYN_flood攻击，含SYN畸形包、SYN小包等，与此同时，大流量攻击还未停止。后续3天，又发生了几次600G左右攻击，均未对业务造成威胁。

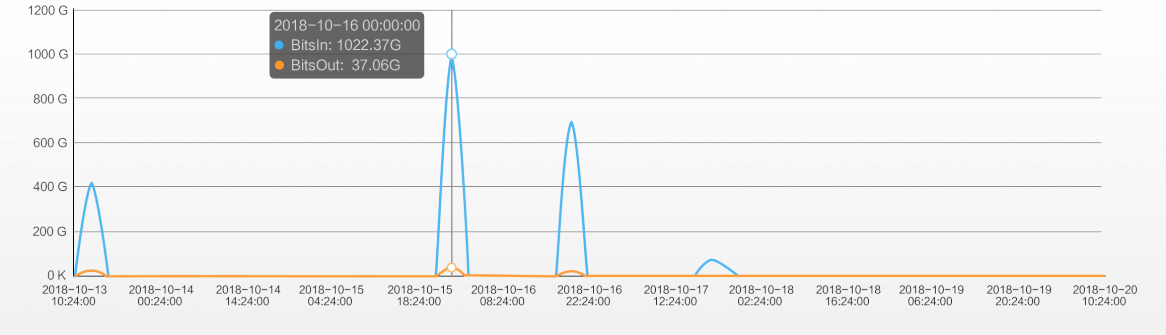


图4-2 2018年阿里云遭受的最大攻击峰值

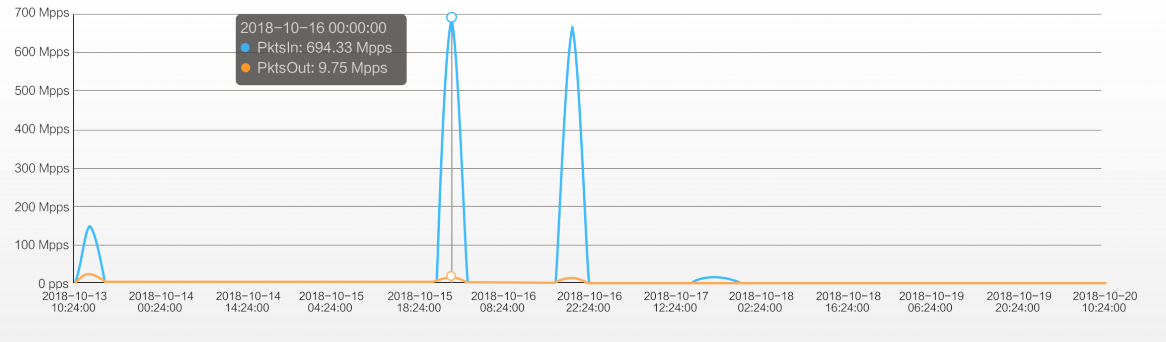


图4-3 2018年阿里云遭受的最高包速率峰值

4.3 连接最大案例

游戏行业一直是DDoS攻击的重灾区，阿里云上的游戏客户同样面临着大流量攻击和连接耗尽型攻击的威胁。2018年7月14日11:47，某游戏客户遭受到大规模的四层连接耗尽型攻击，云盾高防通过智能防护模块检测到四层业务攻击并启动自动防护功能，通过高频次肉鸡处置模块和恶意内容检测模块下发处置，CC攻击流量被完全压制，客户业务恢复正常。收到攻击告警之后，从攻击数据看，黑客动用了20万+的肉鸡资源，攻击手法为建连之后向服务器发起高频率的恶意请求，并带有随机Payload，攻击新建峰值超过了170Wcps。

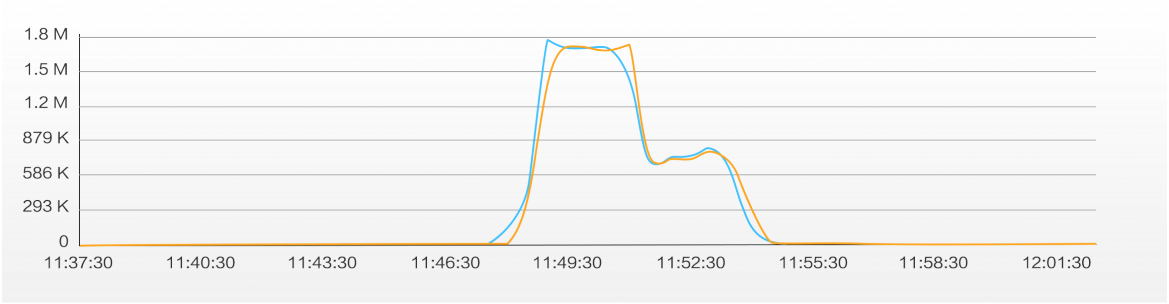


图4-4 2018年阿里云遭受攻击的最高包速率峰值

0000	23	67	47	78	79	4f	33	67	45	56	62	56	32	6c	46	59	#gGxyO3g	EVbV2lFY
0010	5a	64	79	76	53	76	70	6f	7a	42	62	4c	57	62	68	6c	ZdyvSvpo	zBbLWbhl
0020	32	56	6e	4c	70	50	72	31	66	50	50	71	71	53	51	63	2VnLpPr1	fPPqqSQc
0030	42	67	78	37	66	61	56	49	53	4c	69	6c	47	30	72	71	Bgx7faVI	SLilG0rq
0040	57	52	51	71	70	65	4c	4f	4f	4b	31	7a	65	32	43	77	WRQqpeL	OOK1ze2C
0050	48	58	33	67	38	66	45	6e	32	48	73	53	44	7a	61	36	HX3g8fEn	2HsSDza6
0060	30	53	70	4b	34	79	61	61	37	42	7a	37	39	46	45	35	0SpK4yaa	7Bz79FE5
0070	4c	30	31	78	54	68	58	52	4b	55	56	70	4c	6a	69	44	L01xThXR	KUVpLjiD
0080	64	64	4f	38	44	36	37	62	74	5a	35	4e	34	45	35	4a	ddO8D67b	tZ5N4E5J
0090	66	7a	4e	6f	74	36	53	67	4b	38	44	4a	67	71	34	62	fzNot6SgK	8DJgq4b
00a0	4e	46	46	41	57	65	77	6b	35	68	47	79	47	55	49	67	NFFAWew	k5hGyGUlg
00b0	51	61	4b	63	43	44	51	42	49	7a	6e	4c	4c	49	50	53	QaKcCDQ	BIznLLIPS
00c0	32	66	42	6d	6f	39	54	62	4e	51	67	36	63	7a	4c	31	2fBmo9Tb	NQg6czL1
00d0	5a	7a	6d	49	6b	44	4f	73	70	55	4a	51	59	52	53	68	ZzmIkDOs	pUJQYRSh
00e0	46	50	68	74	56	79	62	7a	6f	45	6a	30	39	31	68	74	FPhtVybz	oEj091ht
00f0	73	58	4b	46	54	45	68	30	74	68	77	7a	5a	33	72	34	sXKFTEh	0thwzZ3r4
0100	54	41	30	77	5a	52	67	30	6a	49	79	75	74	48	6a	66	TA0wZRg	0jIyutHjf
0110	7a	69	48	50	75	45	41	31	6a	4b	38	5a	6b	48	47	33	ziHPuEA1	jK8ZkHG3
0120	7a	69	31	72	5a	6a	57	7a	6f	4d	41	33	31	73	6e	53	zi1rZjWzo	MA31snS

图4-5 CC攻击Payload

0190	70	56	35	69	53	36	31	77	6f	66	31	4c	78	77	5a	54	pV5iS61w	of1LxwZT
01a0	69	37	32	75	50	77	39	4d	76	71	48	72	72	41	6a	6c	i72uPw9M	vqHrrAjl
01b0	47	36	4e	73	57	34	56	75	35	54	52	75	31	38	62	56	G6NsW4V	u5TRu18bV
01c0	7a	6b	74	45	6c	47	58	30	59	37	34	65	6a	57	59	36	zktElGX0	Y74ejWY6
01d0	62	44	6a	65	61	66	61	46	64	51	46	6d	31	33	4e	37	bDjeafaFd	QFm13N7
01e0	66	7a	67	73	5a	44	7a	4e	4b	59	6b	58	55	79	56	45	fzgsZDzN	KYkXUyVE
01f0	49	4a	4c	61	42	36	48	46	31	67	46	5a	72	59	41	41	IJLaB6HF	1gFZrYAA
0200	70	64	48	4e	51	44	52	69	44	50	56	74	6f	4e	63	63	pdHNQDR	iDPVtoNcc
0210	5a	30	42	69	56	57	31	59	39	37	57	73	57	75	46	44	Z0BiVW1Y	97WsWuFD
0220	4f	62	42	6f	58	5a	4c	54	58	5a	6b	36	53	75	72	55	ObBoXZL	TXZk6SurU
0230	56	33	73	63	46	75	68	30	45	42	49	4d	33	6f	6e	67	V3scFuh0	EBIM3ong
0240	36	79	64	6a	65	55	58	51	76	62	35	5a	49	44	39	71	6ydjeUXQ	vb5ZID9q
0250	31	4c	6b	4e	6a	41	66	6b	6f	31	32	66	61	4a	78	67	1LkNjAfko	12faJxg
0260	57	79	62	47	37	33	4f	62	4b	67	4a	66	46	49	4e	55	WybG73O	bKgJfFINU
0270	71	75	73	62	70	34	6b	42	6d	4c	50	53	4c	71	73	37	qusbp4kB	mLPSLqs7
0280	31	76	6a	7a	73	46	66	46	33	65	52	71	4a	57	4f	77	1vjzsFfF3	eRqJWOw
0290	57	76	7a	4f	30	49	42	79	4b	61	48	51	64	45	5a	67	WvzO0IBy	KaHQdEZg
02a0	73	4d	4c	33	4f	78	62	77	69	78	68	59	59	67	77	55	sML3Oxb	wixhYYgw
02b0	52	69	58	50	49	52	68	33	7a	6d	67	47	6e	6a	34	6d	RiXPIRh3	zmgGnj4

图4-6 CC攻击Payload

4.4 专家观点

DDoS攻击防护的形势在发生着变化。一方面是反射源的治理，防护手段的演进；另一方面物联网大军正逐渐加入到DDoS的这个战场，攻击手法也日趋复杂化，攻守双方的势力一直保持着动态平衡。如何打破这种平衡，赢取这场战争的胜利，阿里云安全专家给出的建议如下：

1.抵抗住第一波攻击，这很重要。从攻防对抗的经验来看，抵抗住黑客的第一波攻击至关重要。如果第一次攻击得手能够给攻击方带来更多信心，反之多次攻占不下，则会使攻击方信心逐渐丧失。通过寻求专业的DDoS防御团队，永远是被攻击者成本最低、最有效的选择。

2.防守方需要有更成熟的流量调度机制和应对方案。DDoS攻击峰值越来越大，不断地刷新记录，这对于防护方是一个严峻的考验。仅仅依靠单个节点来化解动则上T的攻击已经变得越来越不现实。这时就需要新的应对方案和更成熟的流量调度机制，通过近源清洗、流量压制等技术手段，降低威胁，来力保城门不失。

3.防守方需要思考如何更快速地恢复业务。防守方是被动的，因为攻击者永远在暗处。也许通过事后溯源追查能够找到幕后真凶，但是在攻防对抗过程中，我们不清楚攻击者会通过何种方式利用服务的何种弱点发起攻击。这时防守方就需要考虑如何扭转这种被动局面。随着大数据技术的发展，机器学习的引入，也许能够给我们带来一些机会。通过对正常业务进行建模，来快速检测异常，以及采用智能化的技术手段，快速识别恶意行为并进行处置。通过一系列自动化、智能化的手段，快速恢复业务，也是防护方努力的方向。

黑客发起DDoS攻击，往往是通过侵害别人的正当利益，来使得自己获益。阿里云DDoS团队诞生之初就致力于消灭互联网上的DDoS攻击，只有真正的防御住DDoS攻击，才能消灭互联网的DDoS，这也是我们一直努力追求的目标。


阿里云