2015年第三季度
云盾互联网DDoS状态和趋势报告

2015 Q3 YunDun State and Trends of the Internet DDoS Attacks Report

目录

1、执行摘要 4
2、核心发现 5
3、分析与趋势 6
3.1、攻击类型分布 6
3.2、攻击事件 7
3.3、攻击来源分布 7
3.3.1、国家 7
3.3.2、省份 8
3.4、攻击行业分布 9
3.5、攻击时长 9
3.6、攻击峰值 10
3.7、超过300G的攻击次数 10
3.8、攻击流量分布区间 11
4、僵尸网络研究 12
4.1、僵尸网络以及控制端系统 12
4.2、研究发现 14
4.2.1、控制端系统分布 14
4.2.2、僵尸程序平台分布 14
4.2.3、主要僵尸程序 15
4.2.4、攻击时间分布 16
5、案例 17
5.1、攻击概览 17
5.2、攻击分析 18
5.3、总结 20

目录

6、全球DDoS攻击事件 21

6.1、国外DDoS事件 21

6.1.1、Dota Ti5赛事遭DDoS攻击，赛事被迫中断 21

6.1.2、GitHub遭大流量DDoS攻击 21

6.1.3、Linode数据中心遭DDoS攻击 22

6.1.4、Telegram遭受200Gbps DDoS攻击 23

6.2、国内DDoS事件 24

6.2.1、锤子科技手机发布过程中遭受DDoS攻击 24

6.2.2、魅族科技新品发布期间遭受DDoS攻击 24

6.2.2、知乎遭到攻击，网站不可访问 25

6.2.4、台湾“教育部”网站遭DDoS，导致服务中断 26

7、新兴威胁 27

7.1、BitTorrent DDoS攻击的崛起 27

7.2、来自移动终端的请求洪水攻击流量提升 28

7.3、利用恶意网站爬虫（Bad bots）发起请求洪水攻击 30

1、执行摘要

在2015年第三季度中，阿里云安全团队发现中国范围内的互联网DDoS攻击，无论从攻击数量，还是攻击流量（平均）上，均呈上升态势。

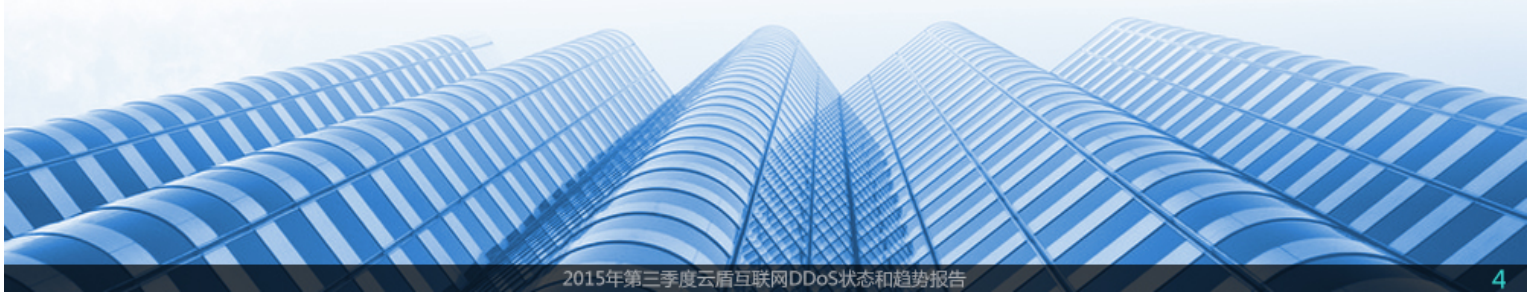
其中流量达到300Gbps以上的攻击次数达到60次。相对于2014年同时期，300Gbps以上的攻击是非常罕见的。

在第三季度中，阿里云安全团队监控到DDoS攻击事件数6万次，月均2万次，攻击总量约为600,000Gbps，峰值攻击为450.2Gbps。CC攻击450亿次，单日最高峰值在50亿次，最大QPS为350万次/秒。

从被攻击者的行业分布来看，游戏和企业的官方网站是重灾区，其他如电子商务、社区论坛，知名媒体等都是攻击者乐意光顾的目标。一个值得关注的现象是，在往年的监控数据中，针对互联网金融行业和电商行业的DDoS攻击并不多，自进入2015年后，对这两个行业的DDoS攻击逐步攀升。在某些新兴行业和竞争非常激烈的行业，DDoS攻击已经成为同行之间竞争，恶意组织敲诈勒索的一个常用手段。

DDoS攻击手段主要包括TCP flood，UDP flood，DNS flood和CC攻击。其中UDP flood中包含了SSDP反射攻击、NTP反射攻击、SNMP反射攻击和DNS 反射攻击。NTP反射攻击随着互联网的治理和宣传环比有下降趋势。在Q2季度的时候，观察到NTP反射攻击占据了所有反射攻击的50%以上，到了第三季度，NTP反射攻击数量下降近一半。

阿里云是国内最大的公共云计算服务提供商。阿里云安全团队依托阿里云云盾系统为用户提供四到七层的所有类型的DDoS攻击防护服务。阿里云安全团队通过对阿里云云计算服务平台、互联网用户和阿里集团系统的安全防护，以及对网络攻击持续的分析与研究，发布第三季度云盾互联网DDoS状态和趋势报告。



2、核心发现

发现1： 第三季度攻击流量持续走高，峰值流量达到450Gbps,日平均流量维持在200-300Gbps左右。

发现2： 从攻击类型的分析来看，攻击者使用最多的是TCP、UDP、SYN、DNS、CC协议攻击，其中UDP占比最多（36%）。

发现3： 持续时间0-30分钟的攻击超过70%，说明攻击者更喜欢使用短时大流量的DDoS攻击来冲击用户业务，而不是选择长时间持续性攻击。

发现4: 攻击者更热衷于20-50Gbps左右的攻击，这个范围内的攻击数量最多。与此同时，300Gbps以上的攻击占总攻击数量的3.3%。

发现5: 由僵尸网络发起的DDoS攻击中，以Windows平台控制端居多。从国内僵尸网络的监控数据发现，广东、江苏、浙江等省份的控制端系统最多。

发现6: 游戏行业是DDoS攻击的重灾区，超过40%的DDoS攻击目标是游戏行业用户。同时，针对互联网金融行业和电商行业的DDoS攻击数量明显上升。

发现7: 阿里云安全团队预测攻击者的攻击流量将持续提升，来自僵尸主机、智能终端以及恶意爬虫的CC攻击将严重影响网站业务，游戏、互联网金融等行业仍将是DDoS攻击的主要目标，同时出于竞争和勒索的目的，在重大活动期间发起攻击将愈发成为攻击者重要选择。

3、分析与趋势

3.1 攻击类型分布

从攻击类型的分析来看，攻击者使用最多的是TCP、UDP、SYN、DNS、CC协议攻击，其中UDP占比最多。从最近几年的攻击趋势来看，DDoS攻击已经演变成为一种资源的对抗的战争，流量型攻击成为最快可以让对方业务不可访问的一种攻击手段。

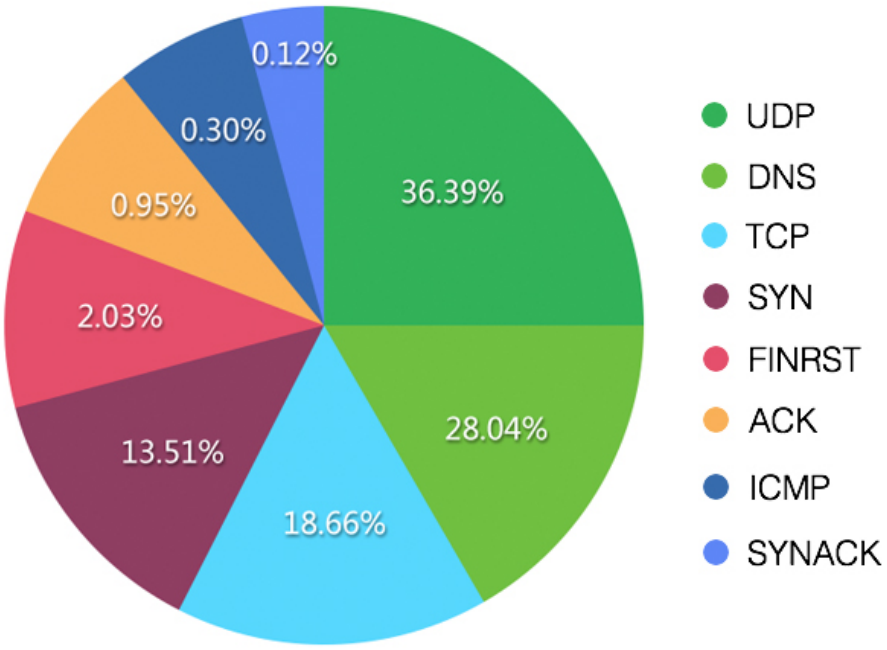


图3-1 DDoS攻击分类

CC攻击的数据可以发现大部分的攻击还是用HTTP GET 的方式。

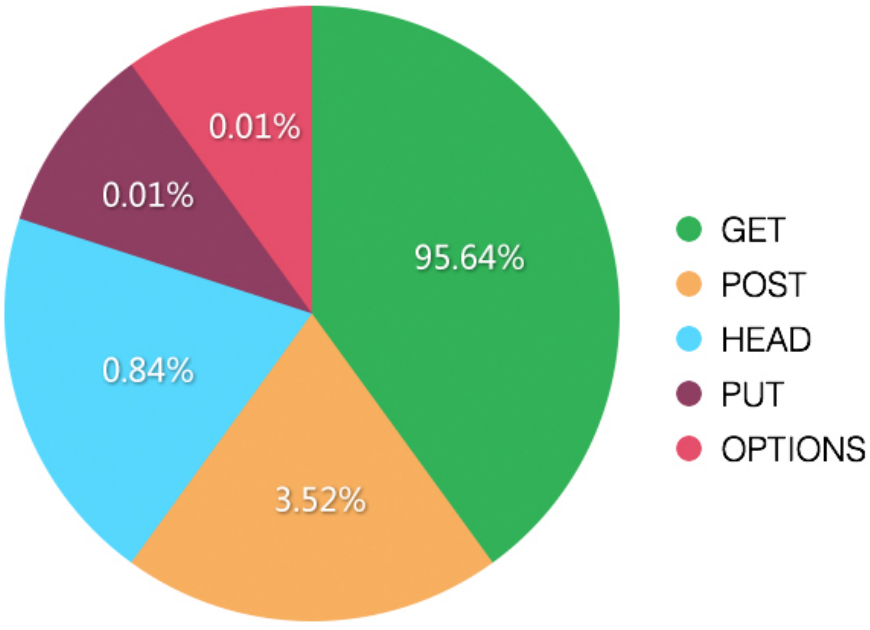


图3-2 CC攻击分类

3、分析与趋势

3.2 攻击事件

第三季度大于50Gbps左右的攻击在进入8月后持续增长，而100Gbps以上的大流量攻击次数比较稳定。

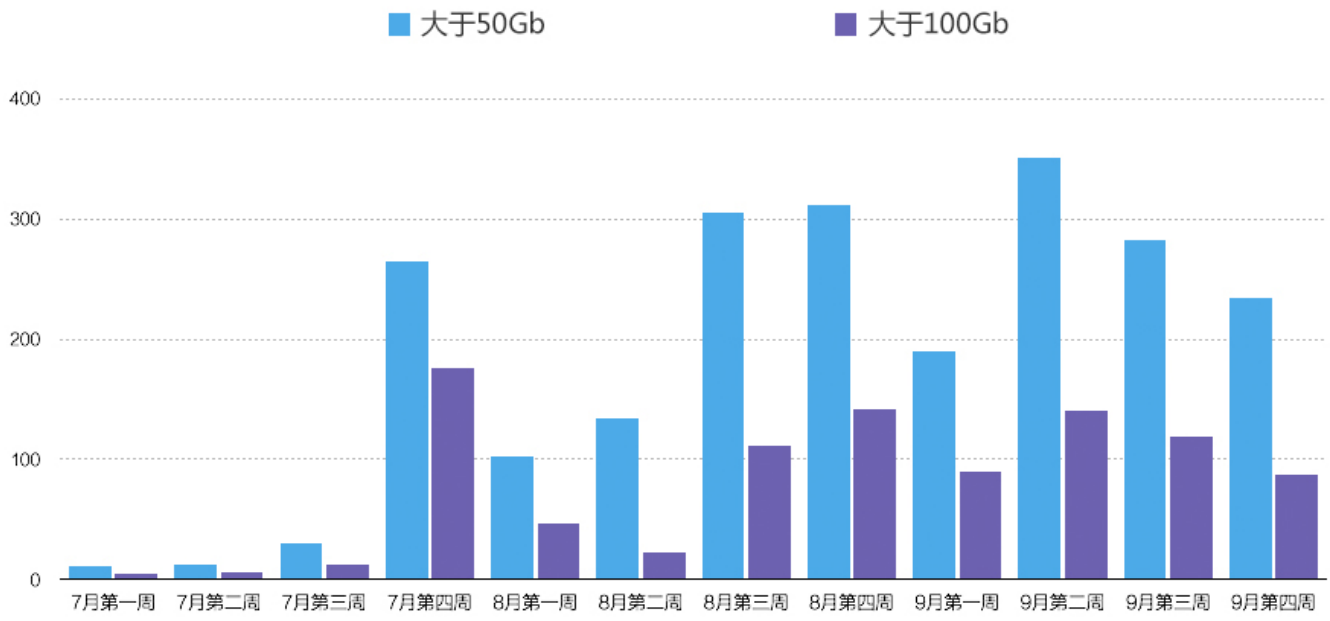


图3-3 攻击事件趋势

3、分析与趋势

3.3 攻击来源分布

3.3.1 国家

攻击来源地在国外的DDoS攻击中，越南、美国和韩国是最主要的三个来源国家。

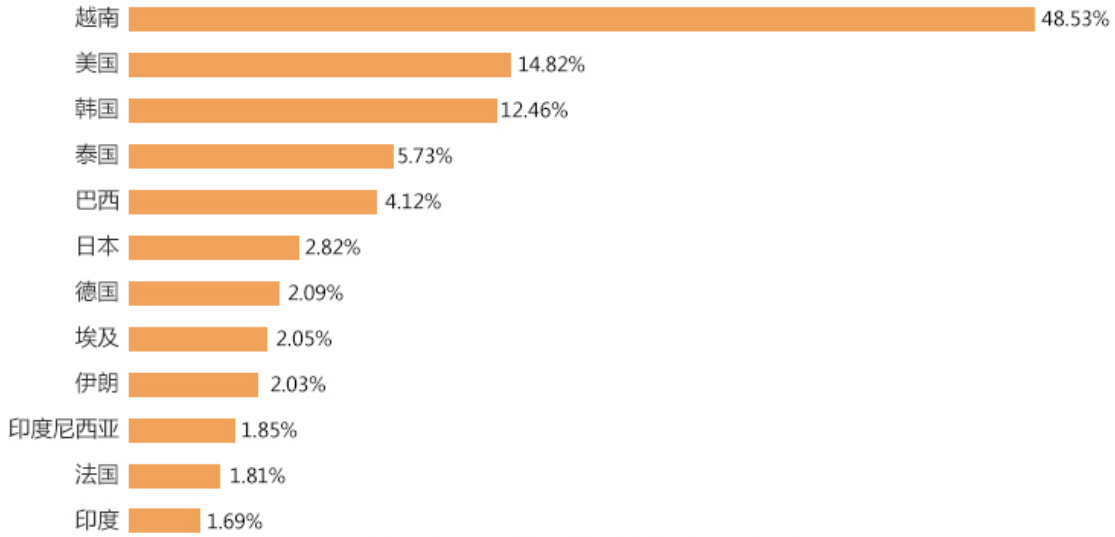


图3-4 攻击来源按国家分布（国外）

3.3.2 省份

来源于国内的DDoS攻击，排名最为靠前三个省份分别是广东、浙江和山东。

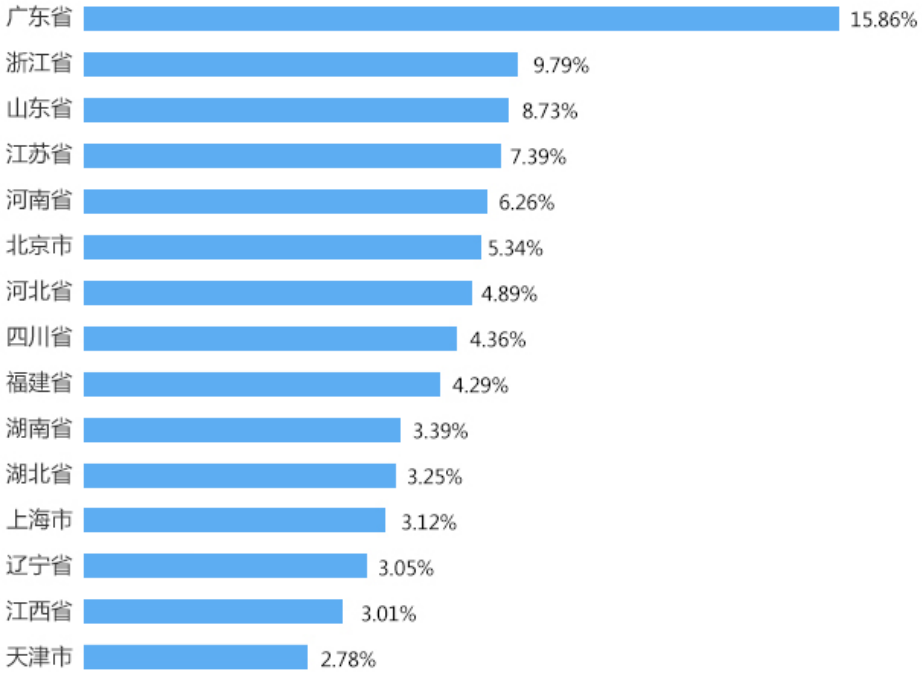


图3-5 攻击来源按照省分布（国内）

3、分析与趋势

3.4 攻击行业分布

从被DDoS攻击骚扰的行业来看，游戏行业遭受的威胁最大。

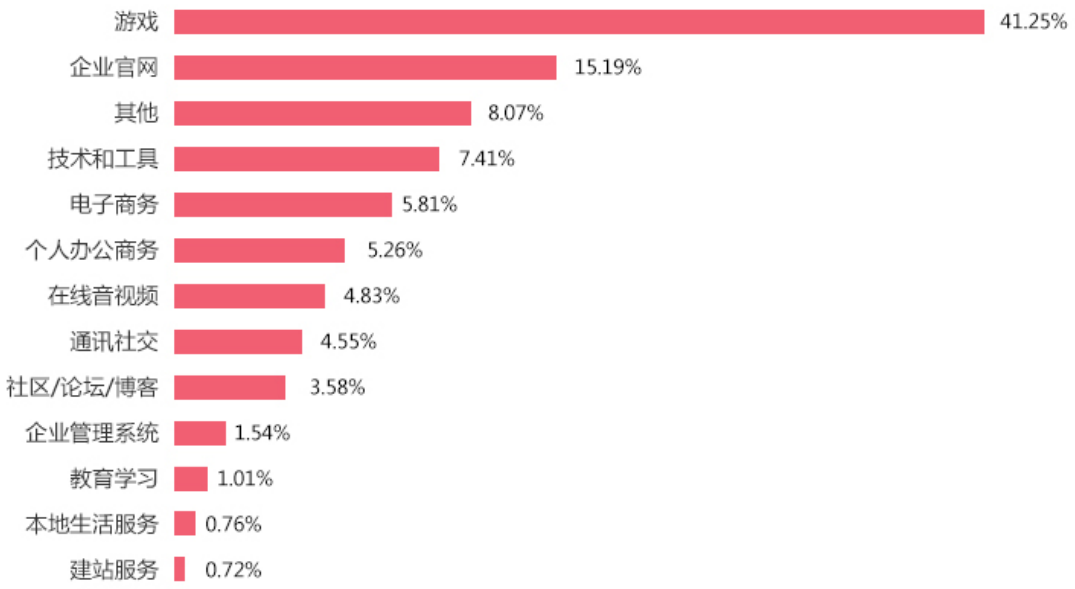


图3-6 攻击按照行业分布

3.5 攻击时长

阿里云云盾对于攻击事件的定义依据两个因素：

1. 阈值因素
2. 流量成分因素

其中，阈值因素主要依据用户预先设置好的DDoS防御阈值（如CC阈值），超过阈值将被视为DDoS攻击发生。流量成分因素主要依据用户通常情况下流量的平均水平构成，如果在某一时刻流量超过平均水平，同时流量构成中出现异常，如大量SYN数据包，则被视为DDoS攻击发生。

在第三季度，攻击者攻击持续时间在0-30分钟的数量超过总数的70%。说明攻击者更倾向在短时间内达到攻击的目标，而不是长时间持续攻击。

3、分析与趋势

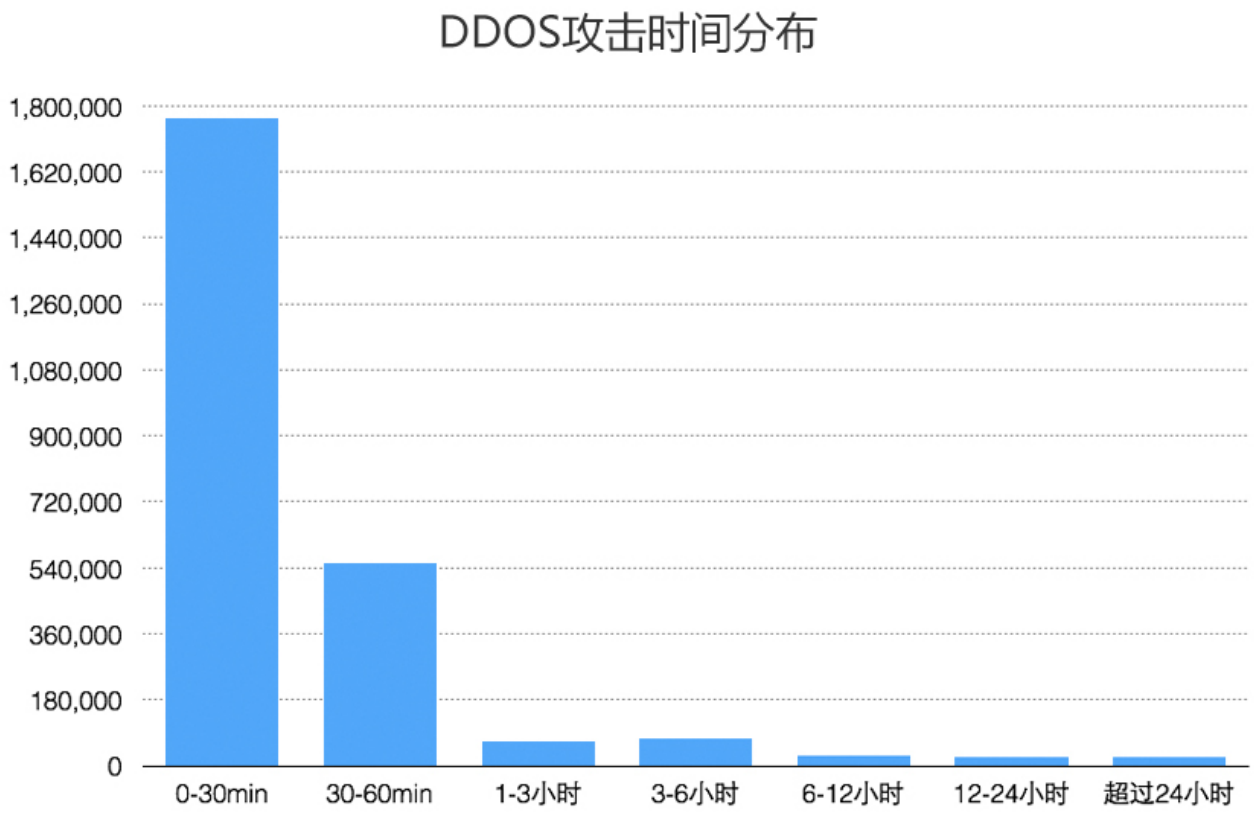


图3-7 攻击时长分布

3.5 攻击峰值

在第三季度，峰值流量为450.23Gbps。

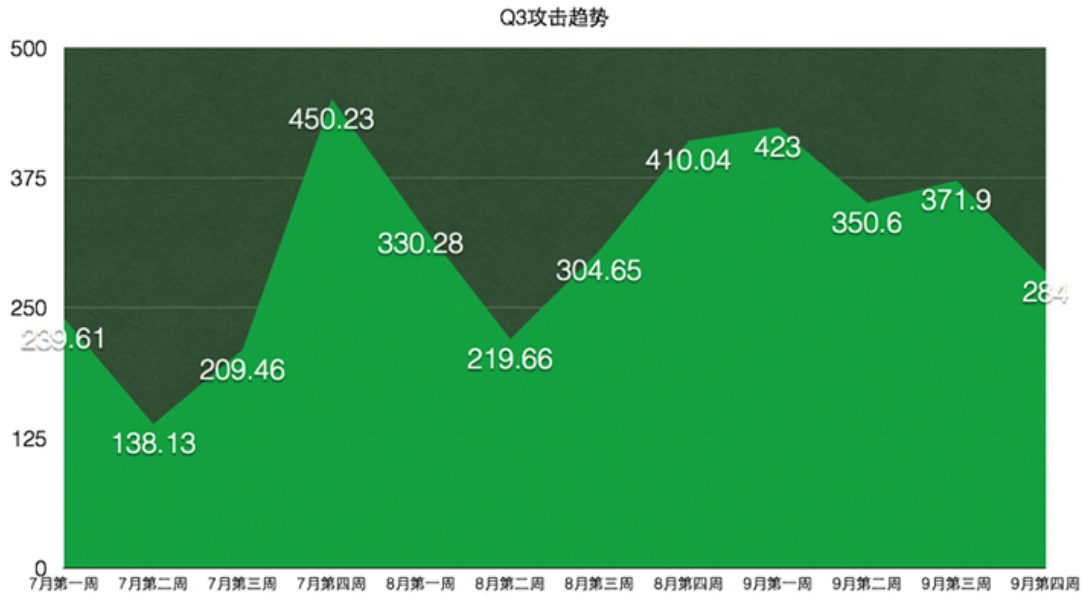


图3-8 攻击峰值分布

3.7 超过300G的攻击次数

在第三季度，超过300Gbps的攻击总数达到60次。

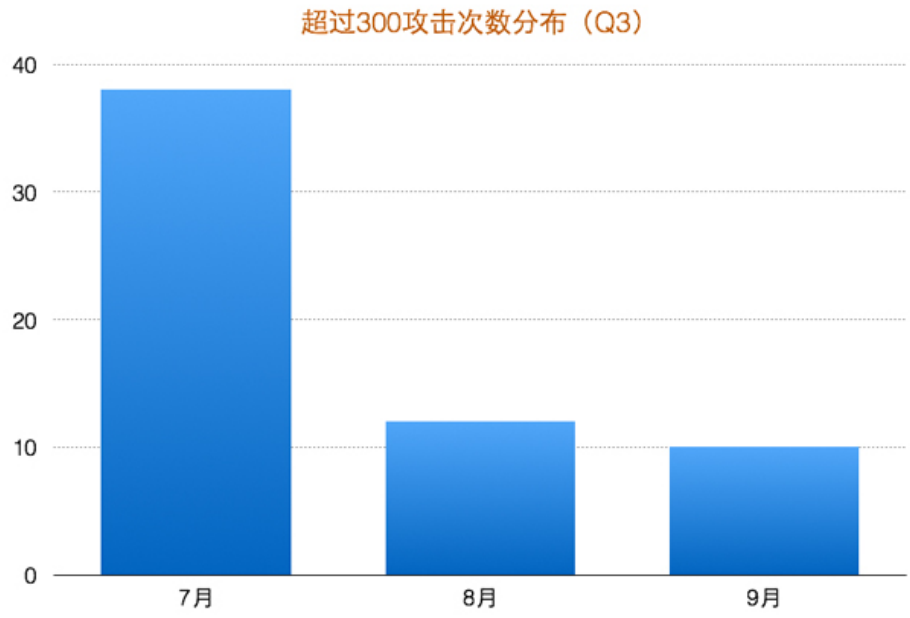


图3-9 大流量攻击次数分布

3.8 攻击流量分布区间

从攻击流量分布的角度上来说，20-50Gbps的攻击数量最多。

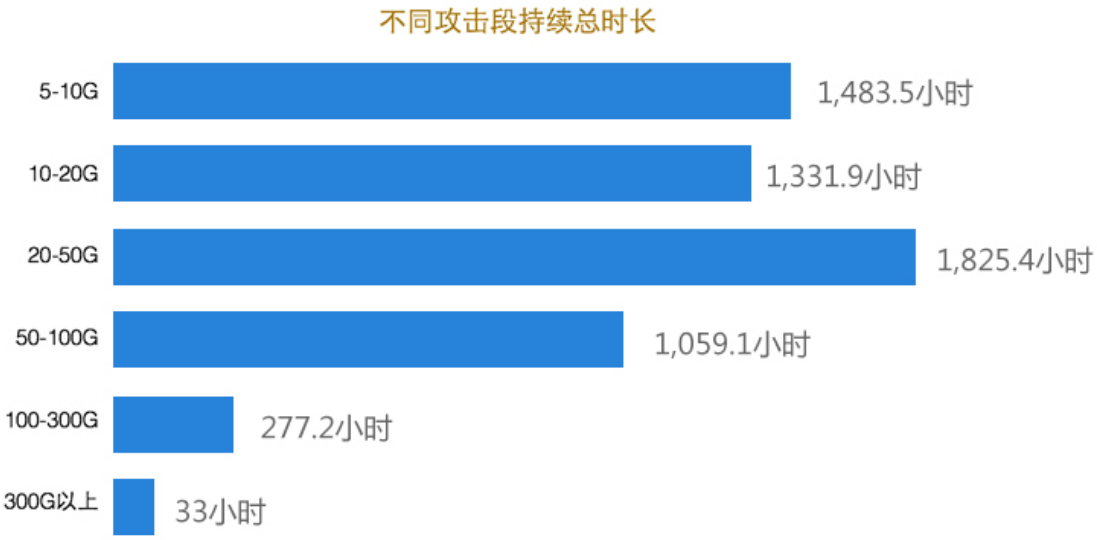


图3-10 大流量攻击次数分布

4、僵尸网络研究

依托阿里云安全团队的持续跟踪与研究，获得了包括DDoS威胁形势、攻击类型及黑产行业方面的大量威胁情报。

在2015年第三季度，阿里云安全团队有针对性地对DDoS控制端系统（Command & Control system, 或 C&C服务器）展开深入研究。

4.1 僵尸网络以及控制端系统

僵尸网络为DDoS的壮大和日益泛滥提供了充足和可靠的资源和手段。由成千上万个人计算机、服务器以及移动设备组成的僵尸网络为DDoS 攻击提供了所需的计算资源和带宽，对互联网造成了极大的危害。

最为传统的DDoS攻击利用僵尸主机（英文：Zombies，俗称“肉鸡”）组成僵尸网络来发起。“肉鸡”是指中了木马，或者被一些人留了后门的计算机，成为“肉鸡”的计算机可以被黑客远程操控。“肉鸡”的存在多由于用户系统存在各种脆弱性导致，系统一旦被入侵，黑客可获得控制权。黑客在这些“肉鸡”所有者不知情的情况下，发起对既定攻击目标的攻击。

4、僵尸网络研究

在僵尸网络的框架中，最为重要的一个组成部分是控制端系统，如下：

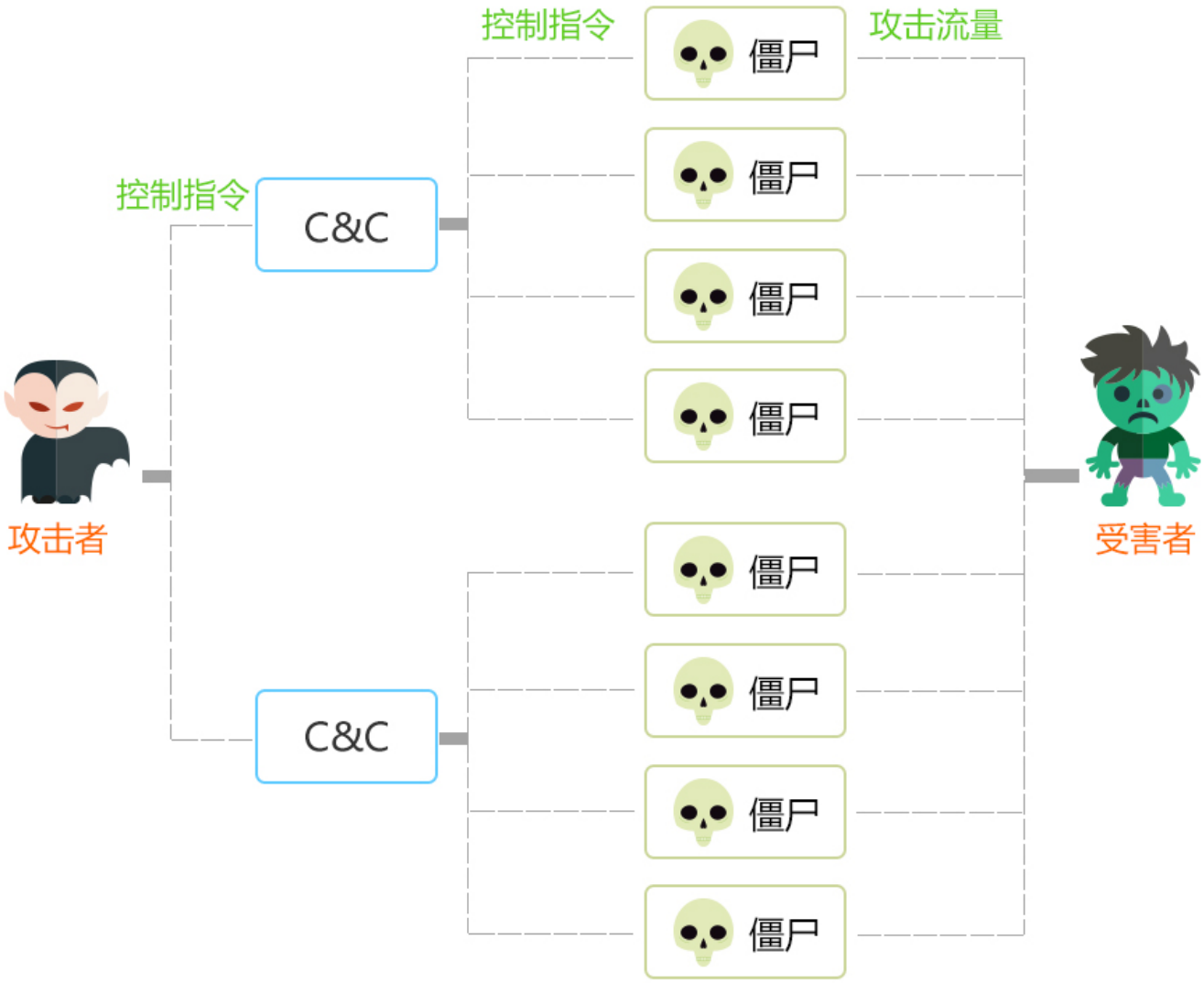


图4-1 典型的僵尸网络框架

控制端系统一方面接收来自黑客的攻击控制指令，同时负责将控制指令下发到成千上万的僵尸主机上，然后由僵尸主机依据控制指令中的信息统一发动针对受害者系统的DDoS攻击。

因此，通过对控制端系统的研究可以了解僵尸主机分布、攻击目标、行为、手段、工具／程序等重要威胁情报信息。

4.2 研究发现

4.2.1 控制端系统分布

控制端系统在中国国内的分布广泛。其中，主要分布区域在中国的南方地区。

排名前三的省份是江苏、广东和浙江，分别占到17%，16%和15%。具体分布下图所示：

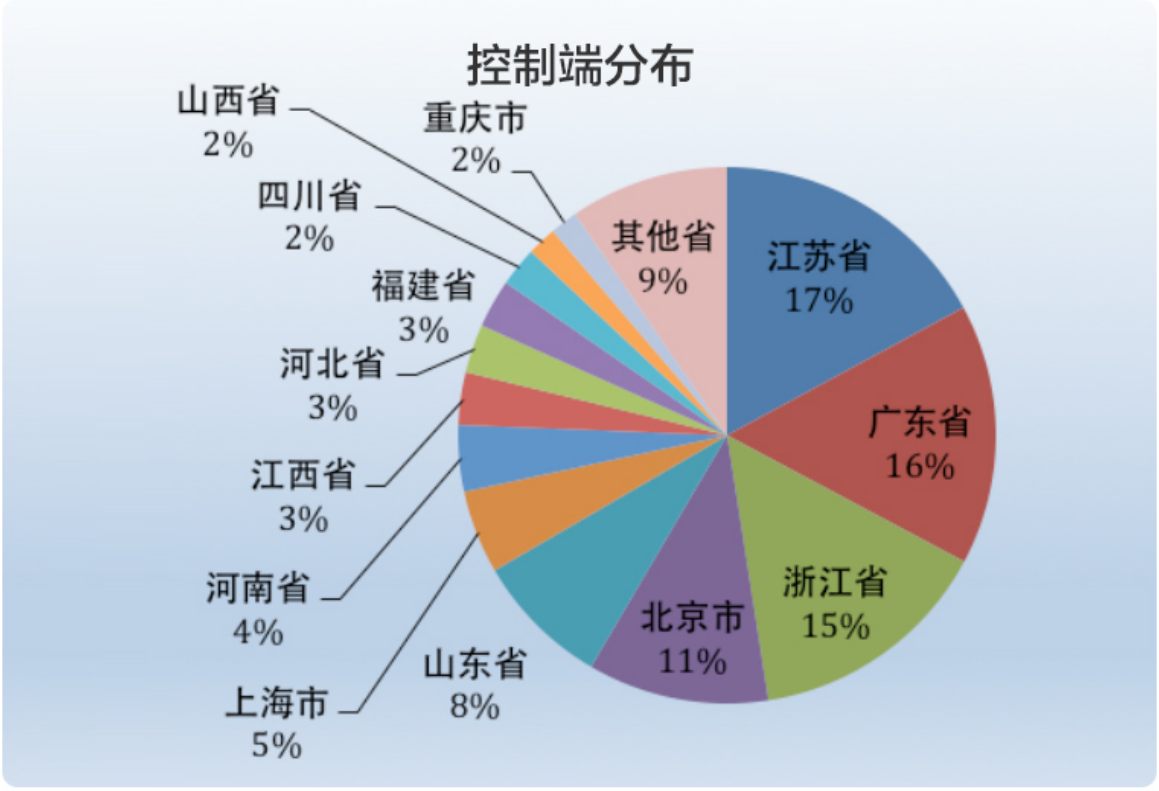


图4-2 控制端分布

4.2.2 僵尸程序平台分布

在僵尸网络中，主要通过控制端系统下发的僵尸程序对僵尸主机进行控制和展开攻击。

4、僵尸网络研究

目前主流的DDoS僵尸程序表现为功能齐全，专业度很高，变种多样化等特点，覆盖Windows、Linux、MIPS和ARM平台，受控“肉鸡”系统已涵盖PC、服务器、智能设备、家庭路由器等多种设备。

通过对攻击程序的分析，近一半（43%）的僵尸程序基于Windows平台，基于Linux平台的僵尸程序占比36%。

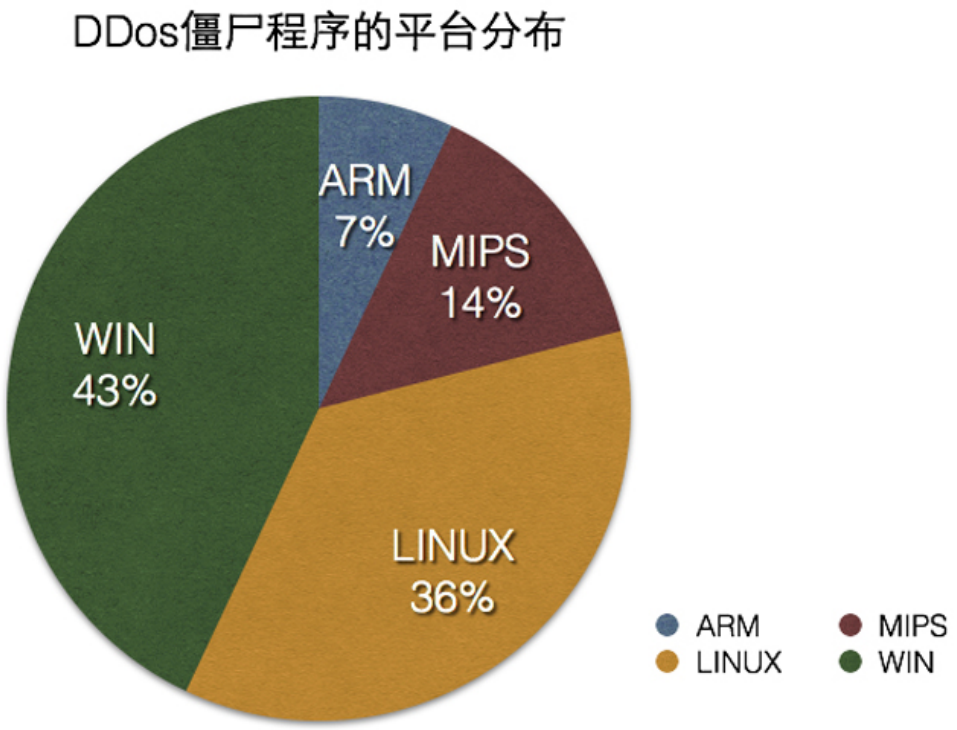


图4-3 DDoS僵尸程序的平台分布

4.2.3 主要僵尸程序

根据威胁情报关联分析，我们发现Top5的僵尸网络程序分别是BillGates，661，Dres，sAE和Xor。其中BillGates和661最为流行，两者之和超过总数的50%以上。

4、僵尸网络研究

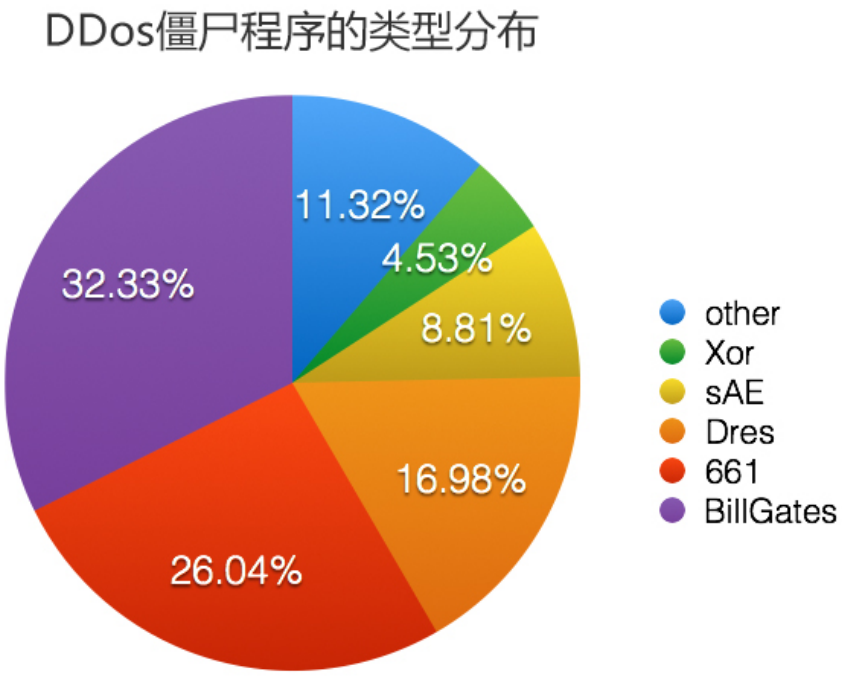


图4-4 DDoS僵尸程序的类型分布

4.2.4 攻击时间分布

发现到DDoS攻击事件的时间分布如下所示：

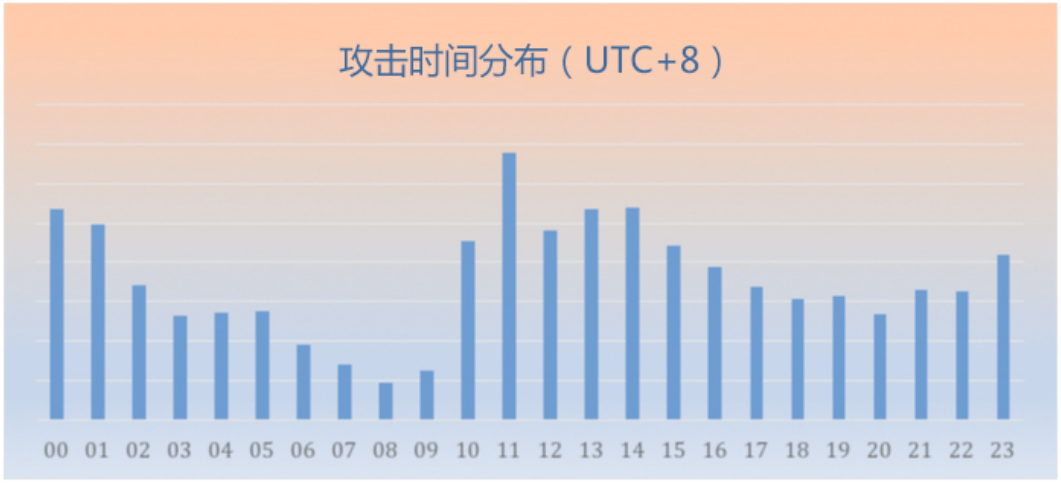


图4-5 攻击事件的时间分布

黑客攻击的高峰时间段为：23点至次日凌晨1点，上午11点至下午14：00。阿里云安全专家推断这两个高峰的形成与网络游戏以及电子商务的业务高峰具有一定的关联性。

5、案例

2015.7.2上午10点开始到下午15点结束，阿里云云盾成功防御黑客对阿里云某P2P金融用户的DDoS攻击。

黑客全天总攻击量达到了20亿次请求，峰值350万 QPS，真实源访问量达到7Gbps，相当于350万的用户在同一时间涌向网站。攻击者此次主要的攻击目标为网站的门户页面和资源页面。一方面从攻击行为上看，无论是攻击目标还是攻击手段均相对固定，说明攻击者并没有对网站目录和页面做过多细致研究。另一方面从过程来看，黑客在短时间组织如此大规模的僵尸网络，说明攻击一方具有丰富的攻击资源。因此，阿里云安全团队认为此次攻击应该是出于商业竞争的目的。

5.1 攻击概览

攻击事件	“72”事件
攻击时间	2015年7月2日
攻击峰值	350万QPS
攻击类型	DDoS攻击（CC攻击）
攻击特点	黑客组织大量僵尸主机频繁请求网站页面
攻击源数量	约10万僵尸主机
攻击主要来源	天津、北京、广州等城市
CC攻击请求（拦截）总数	2,241,359,585次

表5-1 攻击概览

5.2 攻击分析

攻击者从上午10点开始针对网站开始发起攻击，出现两次波峰分别在上午10点30和下午12点30左右。攻击者一开始的攻击即触发预置防护算法，攻击IP被大量加入七层黑名单。从访问情况看，网站业务正常。

12:30的时候出现一股超大流量的CC攻击。从流量日志来看，请求源均为真实访问源。高防安全专家参与与攻击者的对抗。通过溯源、定位和数据包分析，找到攻击特征，攻击被成功压制。

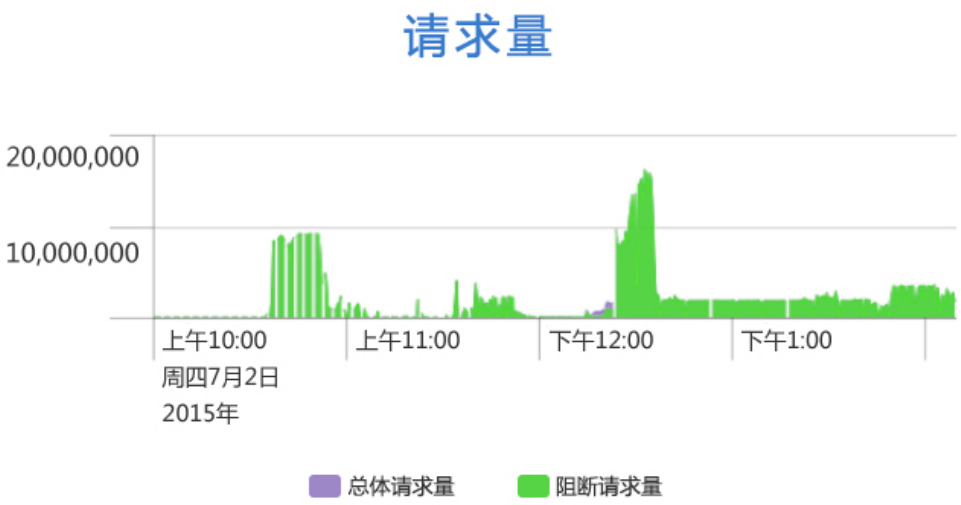


图5-1 攻击请求变化

从攻击源请求的分析来看，90%的请求目标集中在首页，说明攻击者事先并没有做太多的准备和分析工作，推测是接到了攻击需求即开始发流量，涉嫌地下交易。

5、案例

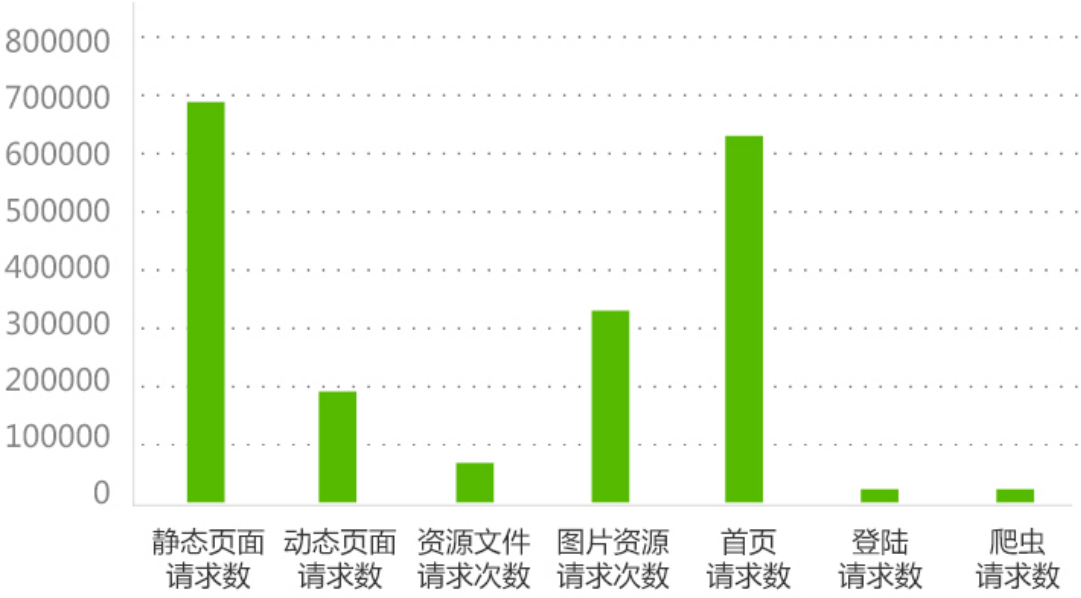


图5-2 源IP请求分布

通过行为分析，得到攻击特征如下：

1) 攻击聚焦首页；
2) 攻击ip在攻击的过程中,为了接近真实主机，攻击者伪造了UA字段和cookie；
3) 攻击IP大部分会持续的进行攻击，持续时间在2个小时左右。

5、案例

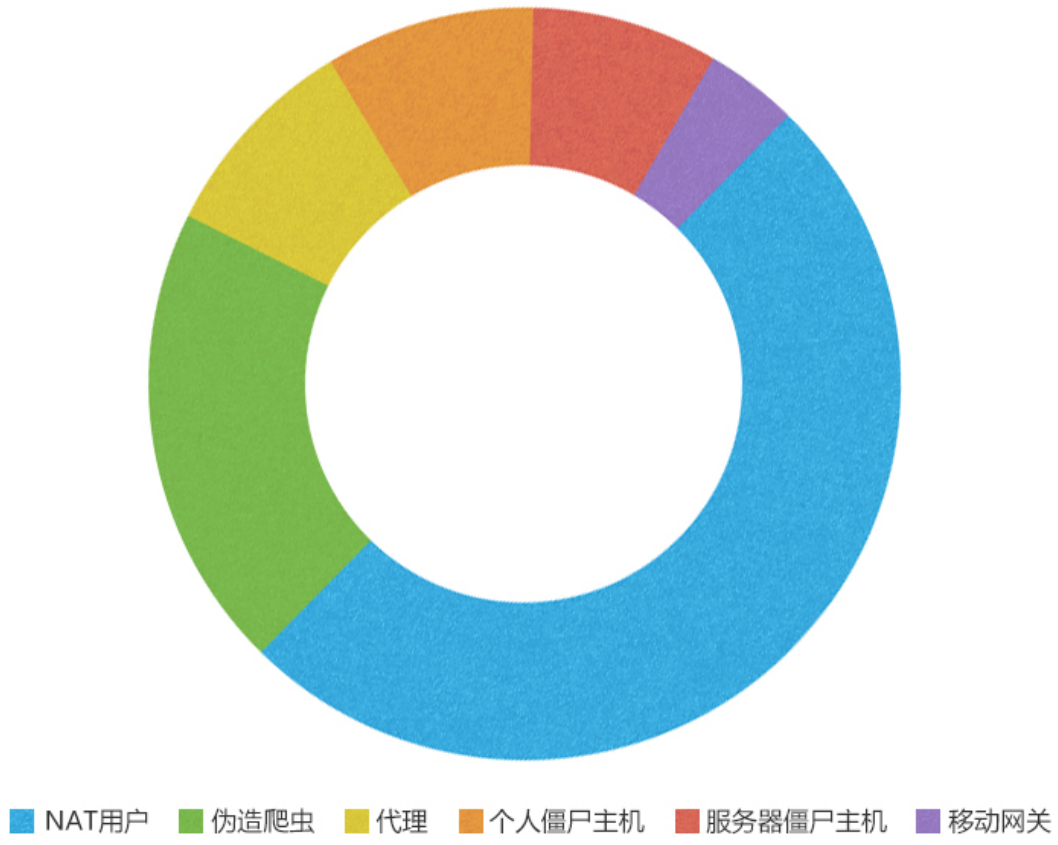


图5-3 攻击IP请求分布

这次攻击事件中服务器僵尸主机占了很大的比重，说明攻击组织者为了获取高性能的攻击资源，利用数据中心机房的服务器发起攻击。

5.3 总结

在本次DDoS攻击事件中，从攻击的方式可以看出，攻击者希望通过对网站的大规模请求来使网站服务瘫痪，攻击量非常大，达到了国内大部分防护厂商设备的性能瓶颈。

从攻击的目标来看，攻击者希望对网站的首页进行突破。同时，攻击源IP分散，说明攻击者很可能使用的是自动化工具。

在整个过程中，云盾高防系统成功防御了黑客攻击，保存了大量有效的攻击证据，极大方便了事后数字取证。

6、全球DDoS攻击事件

在2015年第三季度，全球范围内DDoS攻击事件频发。一些重大安全事件进入我们的视野。其中，游戏行业仍旧是DDoS攻击高发的领域。商业竞争是黑客攻击的重要动机。最后，“黑客主义”（hacktivism）事件也在不断挑战政府系统的网站。

6.1 国外DDoS事件

6.1.1 Dota Ti5赛事遭DDoS攻击，赛事被迫中断。

每年一次的Ti世界邀请赛（The International DOTA2 Championships）主赛事在8月4日开赛的第一天，就遇到了DDoS攻击。主办方却不得不暂停了比赛。本届Ti5的奖金已经达到1800万美金，是DOTA2 TI5有史以来奖金最高的游戏赛事。

6.1.2 GitHub遭大流量DDoS攻击

在8月25日，GitHub网站遭到不明动机黑客的大规模DDoS攻击。在GitHub的状态网页上，可以看到橙色以及红色提示信息。

6、全球DDoS攻击事件

August 25, 2015

21:49 CST	**Everything operating normally.**
20:52 CST	**Service has been restored. We continue to monitor the situation closely.**
20:08 CST	**We are restoring service as we mitigate a DDoS attack. Response times may be slower while this work continues.**
19:27 CST	**We are restoring service as we mitigate a DDoS attack.**
19:06 CST	**We are continuing to work to mitigate an ongoing DDoS attack.**
18:38 CST	**The connectivity problems have been identified as a DDoS attack. We're working to mitigate now.**
18:07 CST	**We're continuing to diagnose reports of connectivity problems.**
17:39 CST	**We are investigating reports of connectivity problems.**
00:08 CST	**Everything operating normally.**

图片来源： status.github.com

图6-1 GitHub网站公告

这是自今年以来GitHub.com遭受的第二次严重DDoS攻击，上一次严重DDoS攻击事件发生在今年3月份。

6.1.3 Linode数据中心遭DDoS攻击

在7月25日，Linode美国纽瓦克数据中心遭到DDoS攻击，导致数据包丢失。

6、全球DDoS攻击事件

图6-2 Linode网站公告

6.1.4 Telegram遭受200Gbps DDoS攻击

Telegram公司7月13日在其官方博客上称 ，三天前其处于亚太区的服务器遭受大规模DDoS 攻击，导致亚太地区的用户出现应用不可访问的情况。据Telegram宣称，攻击流量一度达到200 Gbps，攻击的主要来源是上万台服务器，黑客主要攻击方式是一种新型SYN Flood。

6、全球DDoS攻击事件

6.1 国内DDoS事件

6.2.1 锤子科技手机发布过程中遭受DDoS攻击

8月25日晚，锤子科技手机新品牌“坚果”发布过程中，其电商网站受到了大规模的DDoS攻击，导致用户的购买过程受到影响。

图6-3锤子科技遭到DDoS攻击

6.2.2 魅族科技新品发布期间遭受DDoS攻击

魅族科技在9月23日凌晨发布的微博，称其官网在22日晚间19点左右遭受DDoS攻击，峰值流量达到7Gbps。根据随后负责安全防护的阿里云安全团队统计，在9月23日下午的新品发布会期间，再次遭到两轮DDoS攻击，攻击峰值达到40Gbps。DDoS攻击被阿里云云盾有效阻断，业务未受影响。

6、全球DDoS攻击事件

图片来源：新浪微博

图6-4魅族科技遭到DDoS攻击

6.2.3 知乎遭到攻击，网站不可访问

8月5日，著名社区网站知乎遭到外部攻击，导致网站用户不可访问。黑客可能采用了DDoS攻击的手段。

图片来源：新浪微博

图6-5知乎网站不可访问

6、全球DDoS攻击事件

6.2.4 台湾“教育部”网站遭DDoS，导致服务中断

据台湾《中国时报》报道，全球最大黑客组织“匿名者”的亚洲支部从7月31日晚起对台湾“教育部”网站发动两波DDoS攻击，导致网站瘫痪超过14小时。黑客攻击的背景是日渐激烈的台湾课纲微调争议。

图片来源：taipeitimes.com

图6-6台湾课纲事件

7、新兴威胁

7.1 BitTorrent DDoS攻击的崛起

在2015年第三季度，利用BitTorrent协议脆弱性进行分布式反射拒绝服务攻击的黑客行为引人瞩目。

分布式反射拒绝服务攻击又称DRDoS攻击（Distributed Reflection Denial of Service），其原理是黑客伪造成被攻击者的IP地址，向互联网上大量开放特定服务的服务器发起请求，接收到请求的那些主机根据源IP地址将响应数据包返回给受害者。下图是典型的DRDoS过程：

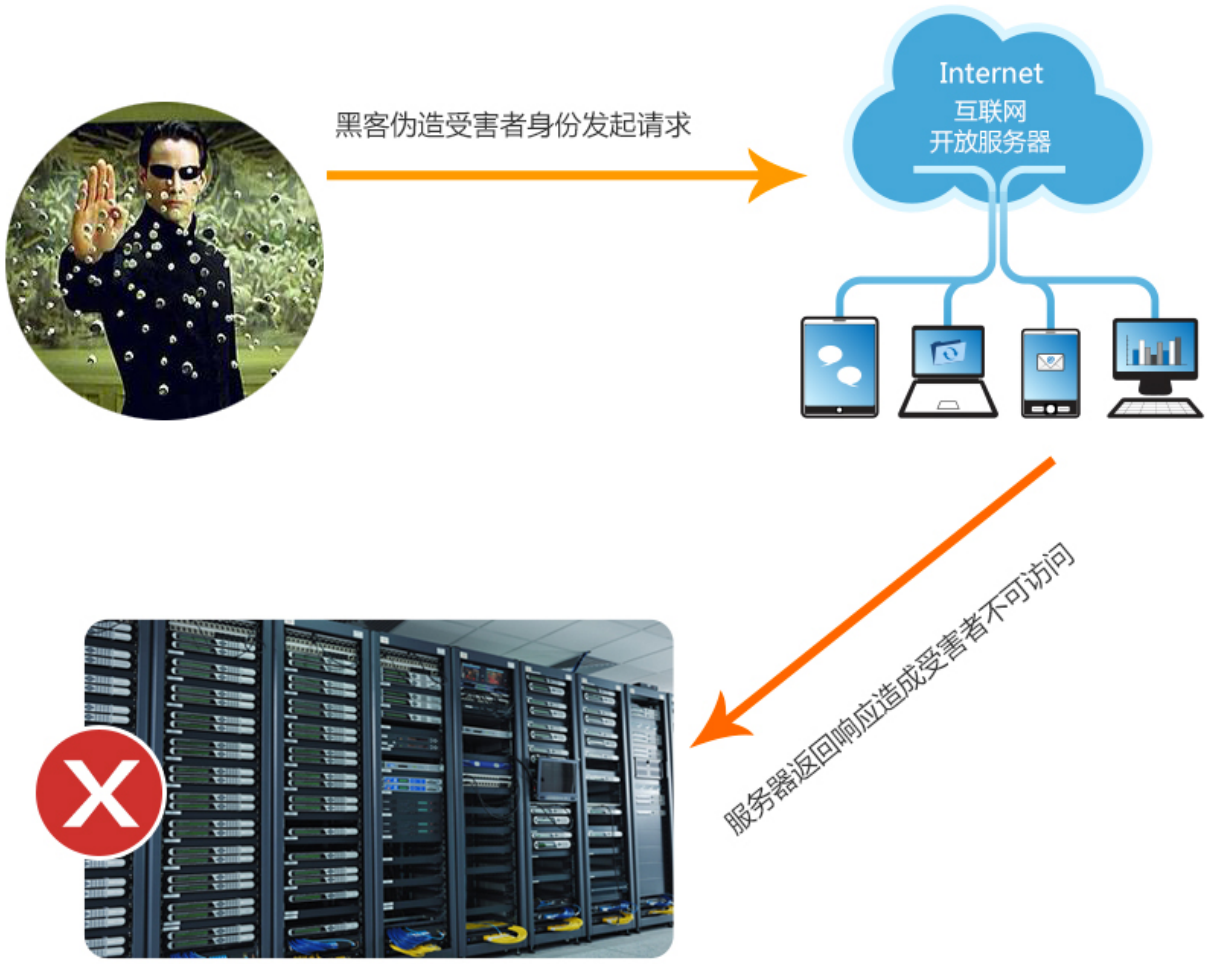


图7-1 分布式反射拒绝服务攻击示意图

7、新兴威胁

黑客往往会选择那些响应包远大于请求包的服务来利用，以较小的流量换取更大的流量，获得几倍甚至几十倍的放大效果。一般来说，可以被利用来做放大反射攻击的协议包括DNS、NTP、SNMP、Chargen以及SSDP等。

根据英国城市大学（City University London）研究发现，BitTorrent协议族可以被黑客利用用来发起分布式反射拒绝服务攻击。具体而言，攻击者可以利用BitTorrent协议的微传输协议（uTP）、分布式哈希表（DHT）、消息流加密（MSE）和BitTorrent Sync（BTSync）。同时，根据城市大学的实验揭示，攻击者能够利用BitTorrent协议获得放大50倍的效果，在采用BTSync协议下可以获得高达120倍的放大效果。

阿里云云盾安全团队的研究发现，在第三季度中多次出现黑客利用BitTorrent协议发起DDoS攻击的事件。对此阿里云安全团队将保持关注。

7.2 来自移动终端的请求洪水攻击流量提升

伴随移动互联网和IoT的发展，越来越多的互联网流量来自Android和iOS移动终端以及包括摄像头、家用路由器等智能终端设备。一方面，大多数移动设备和智能终端缺乏安全保护，另一方面，设备本身的带宽和处理能力在不断提高，使得移动终端逐渐成为攻击者的理想攻击利用平台。

以Android为例，由于发布平台的开放性，很多非官方发布平台，包括论坛和社区，成为黑客首选的恶意程序发布媒介。黑客往往将编写好的恶意程序（往往采用对现有APP重新编译打包的方式），上传到网站上发布。用户下载带有恶意代码的APP，就有可能成为黑客发动DDoS攻击的“肉鸡”。

7、新兴威胁

阿里云云盾安全团队的研究发现，在第三季度中，针对WEB业务和移动APP的请求中，由移动终端发起的请求占了很大比重，主要体现为通过移动端发起CC攻击，以及刷单和刷好评等。

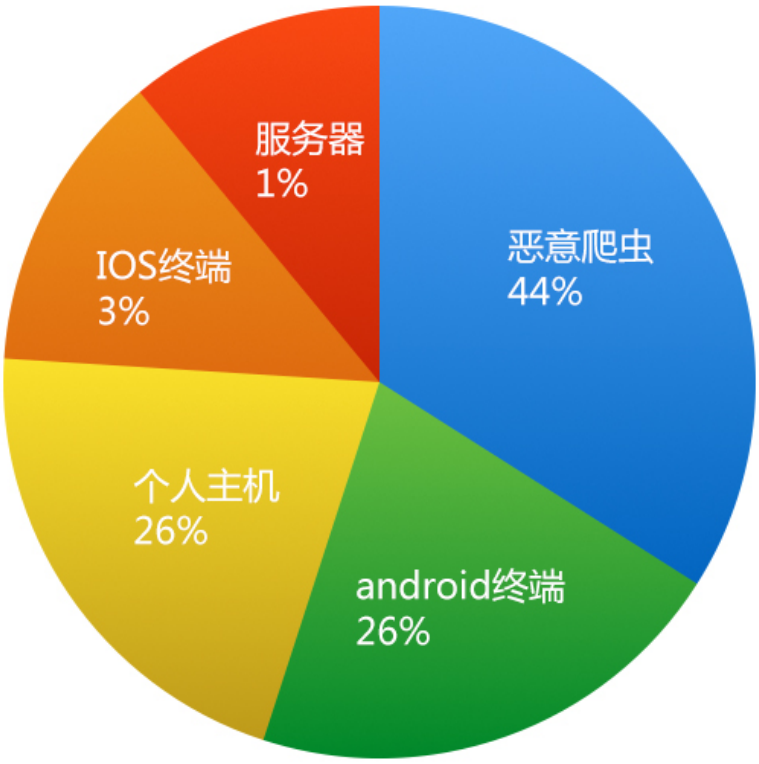


图7-2 攻击源终端分布

7.3 利用恶意网站爬虫（Bad bots）发起请求洪水攻击

网络爬虫（又被称为网页蜘蛛，或网络机器人），是一种按照一定的规则，自动地抓取网站信息的程序或者脚本。

根据Incapsula在2014年12月发布的网络爬虫研究报告《Bot Traffic Report》中，互联网56%的网站访问流量来自于网络爬虫，其中29%是恶意爬虫，27%是正常爬虫。也就是说，从整体角度上来看，网站超过一半的流量是来自网络爬虫。正常爬虫（例如谷歌爬虫、百度爬虫等）对于网站SEO是有促进作用，网站所有者也是欢迎这些正常爬虫的。

恶意爬虫恰恰利用了网站所有者对于正常爬虫的“青睐”，通过伪装成正常爬虫达到欺骗和蒙混过关的目的。黑客主要的手段是模拟搜索引擎的爬虫对目标网站发起扫描，对于被攻击的网站来说，来自伪装搜索引擎的爬虫将很容易地绕过防护系统的防御策略。这些伪装流量将增加网站服务器的负担，在大流量下，甚至可能导致网站服务挂起。

阿里云云盾安全团队在第三季度捕获过伪装为搜狗爬虫的攻击流量。通过对伪装爬虫流量的分析，黑客可以近乎完美地伪造爬虫所有的主要特征字段，这让依据特征进行爬虫流量识别的防护系统形同虚设。

关于阿里云云盾

阿里云云盾是阿里巴巴集团多年来安全技术研究积累的成果，结合阿里云云计算平台强大的数据分析能力，为互联网用户提供DDoS防护、CC攻击防护、云服务器入侵防护、WEB攻击防护、弱点分析、安全态势感知、渗透测试、信息内容安全检测及管控等一站式安全服务，帮助互联网用户轻松应对各种攻击、安全漏洞问题，确保云服务稳定正常。

联系我们：

官方微博：

新浪微博：　阿里云　　阿里云安全

官方微信：

微信公众号：阿里云　　阿里云安全

网站：

http://www.aliyun.com/yundun/ddos