黑镜调查

# 深渊背后的真相之

# DDoS威胁与黑灰产业调查报告


云鼎实验室
YUNDING LAB

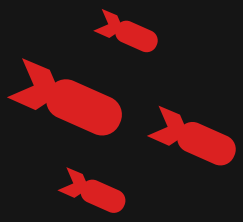
FREEBUF
WWW.FREEBUF.COM

# 声明

本报告为 FreeBuf 与腾讯云、腾讯安全云鼎实验室、大禹联合研究成果。报告中所涉及的数据来自腾讯安全云鼎实验室、大禹及网上公开数据，或采取合法技术手段、深度调查、抽样调查等方式获取。由于统计方法不同、视角和数据观察维度不同，与市场实情可能存在一定误差。



本文仅从学术角度做分析研究，任何非法行为都将受到法律严惩。



## 关于 FreeBuf 研究院

FreeBuf.COM 是斗象科技旗下、国内领先的互联网安全新媒体，每日发布新鲜安全资讯、技术剖析，分享国内外热门安全资源，是深受安全从业者与爱好者关注的网络安全网站与社区。FreeBuf 研究院则集结了行业内经验丰富的安全专家和分析师，常年对信息安全技术、行业动态保持追踪，进行专业的安全行业现状和趋势分析。

## 关于腾讯安全云鼎实验室

腾讯安全云鼎实验室，关注云主机与云内流量的安全研究和安全运营。利用机器学习与大数据技术实时监控并分析各类风险信息，帮助客户抵御高级可持续攻击；联合腾讯所有安全实验室进行安全漏洞的研究，确保云计算平台整体的安全性。相关能力通过腾讯云开放出来，为用户提供黑客入侵检测和漏洞风险预警等服务，帮助企业解决服务器安全问题。

# 目录

声明
目录

第一章 概述
1.1 DDoS 概念及种类
1.2 DDoS 现状及趋势
1.3 DDoS 产业链

第二章 DDoS 热点事件与关键技术
2.1 DDoS 热点攻击事件
2.2 DDoS 新颖的攻击技术
2.3 DDoS 关键防御技术

第三章 2018年 DDoS 攻击情况
3.1 DDoS 攻击发生时间段
3.2 DDoS 攻击持续时间
3.3 攻击类型各流量区间分布
3.4 全球 DDoS 攻击目标国家占比
3.5 中国 DDoS 攻击目标各省份占比
3.6 攻击目标行业分布
3.7 僵尸网络 C2 服务器全球分布
3.8 僵尸网络 C2 服务器国内分布
3.9 典型攻击事例

第四章 DDoS 产业链及新变化
4.1 DDoS 产业链
4.2 产业新变化

第五章 安全建议

附录

参考来源

关于报告

# 第一章 概述

## 1.1 DDoS 概念及种类

DDoS 全名分布式拒绝服务攻击（Distributed Denial of Service），将多台设备联合起来作为攻击平台，对一个或多个目标发动拒绝服务攻击，使得攻击威力成倍提高。DDoS 攻击最早可追溯到1996年，这种古老的攻击方式经过近二十年的演变沿用至今。DDoS 攻击素来以成本较低、效果显著、影响深远为攻击者所青睐。目前主流的DDoS攻击方式主要包括传统攻击：ICMP Flood、UDP Flood、SYN Flood、HTTP Flood 等；反射放大攻击：NTP Flood、SSDP Flood、DNS Flood等；及根据攻击目标的特点进行的有针对性的混合攻击。据统计，2018年最流行的DDoS攻击方式包括异军突起的反射放大攻击、SYN Flood 和 HTTP Flood。

从攻击类型来看，反射放大占比最多，约为55.8%。 Memcached 作为2018年三月以来的新兴反射放大力量，迅速被 DDoS 黑产界利用，其在整体的占比中也相当大。反射放大占比如此之多的一个原因是 DDoS 黑产的自动平台化，即无需人工干预，完全自动流程可完成攻击的所有操作。

SYN Flood 排名第二，一直是 DDoS 的主要攻击手法。随着 DDoS 黑产的平台化，SYN Flood 的载体也发生了改变，由海量的肉鸡渐渐转移到了发包机上（以伪造源 IP 的 SYN Flood 为主）。

HTTP Flood 作为7层攻击的主要方式，因为要建立完整的 TCP 连接，不能够伪造源 IP，所以还是以肉鸡侧发动攻击为主。但经调查发现，HTTP Flood 也开始向代理服务器和发包机发展。

## 1.2 DDoS 现状及趋势

互联网大潮的冲击之下，人工智能、云计算、大数据、物联网等新技术愈发成熟，社会及企业数字化转型进入关键阶段，网络空间安全面临的威胁也在不断变化升级。作为影响最深远的安全威胁之一，DDoS 攻击仍然活跃。

DDoS 攻击流量峰值每年都不断地被超越，上半年的一起 Memcached DDoS 攻击，其峰值1.7 Tbps 达到了一个新的高度。随着各行各业的互联网化，DDoS 的攻击面也越来越多。游戏行业因其日流水量最大、变现快，一直站在利益的风口浪尖上，当仁不让地成为 DDoS 首选的攻击目标，也是2018上半年各行业中遭受攻击最多的行业。值得关注的是在医疗、物联网、教育等传统行业互联网化后，也遭受到了不同程度的攻击，且呈上升的趋势。

## 1.3 DDoS 产业链

高额利润催生精细化分工，DDoS 攻击也不例外。早年传统 DDoS 攻击往往由黑客一人承担工具开发、Bot 传播、接单、攻击实施，而新兴的 DDoS 服务则完成了多环节自动化发展，页端 DDoS 攻击平台已成为当下主流，成单率更高、响应速度更快、攻击效果更强。

在资源不对等的大环境下，提升技术能力将成为未来防御 DDoS 攻击的关键。

## 1.4 关键发现

1.异军突起的反射放大攻击在2018年各类 DDoS 攻击中占比高达55.8%。

2.2018上半年一起 Memcached DDoS 攻击，峰值 1.7 Tbps 创造新的历史记录。

3.游戏行业成为 DDoS 攻击的首选对象，其中手机游戏超过 PC 客户端，第一次成为该类别的主要目标。

4.美国依然是全球 DDoS 攻击的头号重灾区，国内 DDoS 被攻击省份集中在江浙、广东等发达地区。

5.DDoS 产业化已经非常成熟，从业者们分工明确，并与其他黑灰色产业存在交集。

6.各种主流的即时通迅工具及主流的网络商城成为 DDoS 攻击的主要发单渠道。

7.暗网 DDoS 及 DDoS 服务平台为行业带来新变化，并有愈发壮大的趋势。

# 第二章 DDoS 热点事件与关键技术

## 2.1 DDoS 热点攻击事件

### 2.1.1 DreamHost

2017年8月24日上午9点20分，黑客利用 DDoS 攻击了网络托管服务提供商和域名注册商 DreamHost，使其 DNS 系统无法正常工作。

有人认为攻击来自于那些反对处罚斯托默网站的人，斯托默网站是一个新纳粹网站。网站原本搭建在 CloudFlare，之后因抗议 CloudFlare 终止了服务。几个小时后，DreamHost 恢复了相关服务。

### 2.1.2 英国国家彩票

2017年9月30日当地时间19:00，不法分子针对英国国家彩票进行了 DDoS 攻击。这次袭击使得彩票网站 www.national-lottery.co.uk 及其移动应用程序离线，导致英国公民无法正常购买彩票。

当地时间23:00，大部分服务都被恢复。但彩票的网站和应用程序继续遇到小故障，直到03:00才完全修复。

### 2.1.3 Electroneum

Electroneum 加密货币公司 ICO 之后，收集了价值4000万美元的比特币和以太币。就在2017年11月2日 Electroneum 推出其移动挖矿程序前夕，公司网站遭受到了大规模 DDoS 攻击。

攻击使得 Electroneum 用户账户被锁定。与此同时，金融市场行为管理局提醒投资者，ICO 不受任何法律保护。

### 2.1.4 波士顿环球报

2017年11月8日美国东部时间15:00，波士顿环球公司遭到了 DDoS 攻击。攻击针对 bostonglobe.com，扰乱了报社的电话和编辑系统。随后，黑客在次日再次实施了攻击。许多波士顿环球员工的工作被迫暂停， bostonglobe.com 无法访问。当公司的互联网服务提供商实施有效的反 DDoS 措施后，服务在下午被修复。

### 2.1.5 GitHub

2018年3月，知名代码托管网站 GitHub 遭遇了 Memcached DDoS 攻击，攻击流量峰值达到1.35 Tbps。短短一周不到，美国一家服务提供商也受到了同样攻击，流量峰值达到史无前例的1.7 Tbps。不法黑客利用 Memcached DDoS 攻击反射放大的特点，凭借其超5万倍的反射放大倍数，刷新了 DDoS 攻击的流量峰值记录。

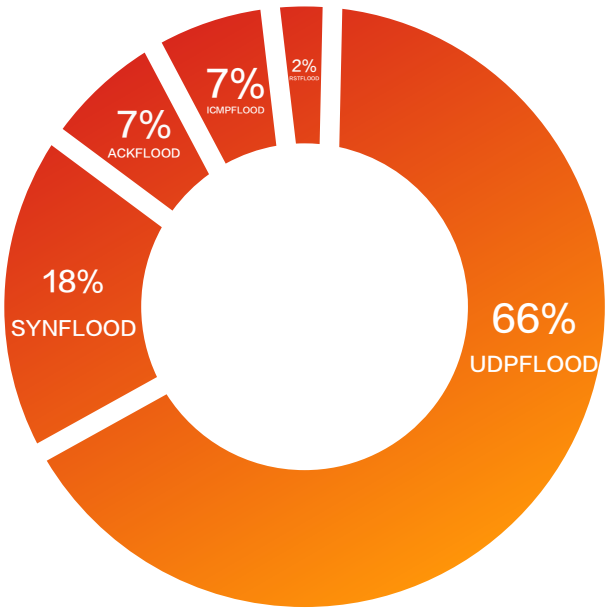
### 2.1.6 育碧

2018年7月，育碧服务器再次遭到 DDoS 攻击，从7月12日开始玩家就遇到了接连不断的游戏登陆问题。虽然育碧在几个小时之后处理了这些问题，但几天之后游戏的连接匹配问题再次发生。

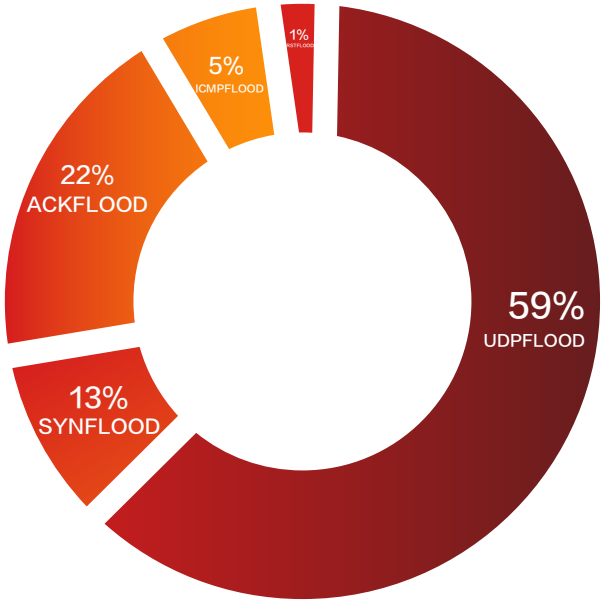
根据育碧官方报告，这次大规模的连接问题是由于他们的服务器受到了 DDoS 攻击，导致许多游戏受到了延迟影响，包括《孤岛惊魂5》、《彩虹六号：围攻》、《荣耀战魂》、《幽灵行动：荒野》以及《极限巅峰》。

## 2.2 DDoS新颖的攻击技术

2018年上半年的 DDoS 攻击流量类型统计结果显示，UDP Flood 无论从攻击流量还是从攻击次数来看，都占有绝对的优势。UDP Flood 的主要流量来源于 UDP 反射放大攻击，这些反射放大攻击使用了一些基于 UDP 协议不需要验证的服务器，且接收数据远大于发送数据，攻击者通过伪造源 IP 为受攻击者的 IP， 利用互联网中分布众多的服务器带宽资源发起攻击。




2018上半年攻击流量占比统计




2018上半年攻击次数占比统计

常见的反射放大攻击利用的协议有 SSDP、NTP、DNS、CHARGEN 等，但在与黑客斗智斗勇的过程中，新的方法总是层出不穷，上半年就新出现了利用 Memcached 协议、IPMI 协议的新型反射攻击，同时还有混合在众多攻击中的 TCP 反射攻击。

### 2.2.1 Memcached 服务器实施反射 DDoS 攻击

提到反射就不得不提新型的反射攻击手段 Memcached 协议利用，它引起了互联网界的一场海啸，其最高攻击流量达到了 1.7 Tbps，云鼎实验室也检测到了高达 1.2 Tbps 的攻击。这种新型攻击手段利用 Memcached 协议默认开启 UDP 11211端口，通过命令执行上传下载 key:value 项的特性，达到理论放大值超5万倍的效果。经过试验验证，受带宽等实际环境的影响，虽未能达到理论值，但可以利用极其低廉的成本和极少数的可利用服务器列表就能达到可观的攻击值，对未添加防护设备的用户来说其影响是及其巨大的。

如今的 DDoS 攻击大多使用反射攻击将流量放大，攻击者并不直接攻击目标服务 IP ，而是通过伪造被攻击者的 IP 向开放某些特殊服务的服务器发请求报文，该服务器会将数倍于请求报文的回复数据发送到那个伪造的 IP（即攻击目标 IP），从而实现四两拨千斤的效果。而黑客们也不断推陈出新，用一些新的反射型攻击达到高达数万倍的放大效果。

Memcached 是一个用于加速网站和网络的数据库缓存系统。攻击者将欺骗请求发送给易受攻击的 UDP Memcached 服务器，然后利用流量淹没目标受害者，从而压倒受害者的资源，使得目标的基础架构过载，无法处理新请求，且常规通信无法访问资源，导致拒绝服务。

### 2.2.2 CLDAP 反射放大类型 DDoS 攻击

CLDAP 攻击技术是一种利用轻量目录访问协议（Lightweight Directory Access Protocol，LDAP）的放大攻击，峰值可以达到 Tb 级别。LDAP 是访问类似 Active Directory 数据库用户名和密码使用最广泛的协议。它基于X.500标准，但更加轻便简单并可以根据需要定制。另外，与X.500不同，LDAP 支持 TCP/IP。

黑客利用 LDAP 协议的漏洞实施攻击可以让放大系数达到46，在特定条件下，峰值甚至能达到55。

攻击者可以从伪造地址（受害人地址）向支持 CLDAP （无连接轻量级目录访问协议）的服务器发送一个请求。当 LDAP 服务器处理请求之后，便会向发送人的地址发送回复。 LDAP 服务器发送的回复内容是原请求内容的数倍，从而形成反射放大

### 2.2.3 Mirai僵尸网络的变种攻击

Mirai 僵尸网络于2016年被发现，10月份其源码泄露，网络上很快便出现了多种 Mirai 变体，包括 Satori， Masuta 和 Okiru。
Wicked Mirai 这个名字来自代码中的字符串，专家发现，与原始版本相比，这个新变种至少包含三个新的漏洞。由于两年前公布了源代码， FortiGuard 实验室的团队看到了越来越多的 Mirai 变体。
最初的Mirai试图强行破坏其他 IoT 设备，而 Wicked Mirai 通过向物联网设备的多个端口（如80、81、8080、8443等）发起 TCP 连接请求以探测危险端口是否开放，一旦端口处于开放状态且连接建立成功，僵尸程序将尝试利用该设备已知漏洞进行攻击，攻击成功后将下载僵尸程序，实现持续的扩散感染。

专家们发现，漏洞利用取决于僵尸程序能够连接到的特定端口：

- 8080端口：NETGEAR DGN1000 和 DGN2200 v1 路由器
- 81 端口：CCTV-DVR 远程代码执行
- 8443端口：NETGEAR R7000 和 R6400 命令注入
- 80端口：受威胁的 Web 服务器中的调用程序外壳

### 2.2.4 IPMI反射

IPMI基于UDP协议，建立远程管理控制服务，默认开放623端口。攻击者可以利用远程管理控制服务使用的命令以及使用 IPMI 的设备自身的接口漏洞执行反射攻击，从目前的监测情况看，虽放大比例只有1.X倍，并未产生大流量攻击，但如果此类设备暴露在互联网中的数目增多，造成的后果依然不可估量。

### 2.2.5 TCP ACK反射

除此之外，TCP ACK 反射攻击也混杂于多种攻击形式中崭露头角。TCP 反射是攻击者伪造受害者的 IP 作为源地址，向互联网上开放 TCP 80/443/8080等常见端口服务的 IP 发送 SYN 包，接受 SYN 包的服务器就会向受害者IP回复 SYN-_ACK包，造成受攻击者网络资源消耗、阻塞、甚至引起服务中断的方法。虽然基

本不存在放大效果，但基于其真实 IP 的原因，穿透性与隐蔽性都十分显著。

## 2.3 DDoS 关键防御技术

下面介绍一些目前应用效果较好的防御手段。

### 2.3.1 IP轮询技术

对稳定性、流畅性以及安全性上要求较高的业务，用户遭受 DDoS 攻击且达到一定峰值时，系统通过 IP 轮询机制，将从IP 池中灵活调取一个新的 IP 充当业务 IP，使攻击者失去攻击目标，以此保证业务在 DDoS 的攻击下正常运转。

### 2.3.2 BGP 高防 IP

当用户应用 BGP 高防 IP 且配置转发规则和域名回源后，此时所有的访问流量都将流经 BGP 高防 IP 集群，通过端口协议转发的方式（支持网站业务和非网站业务）将访问流量转发至源站，同时攻击流量将在 BGP 高防 IP 集群进行清洗和过滤，只会将正常业务流量返回至源站，从而确保源站业务的稳定。

### 2.3.3 运营商过滤

针对反射放大类攻击，都有相同的特点，可以直接在运营商侧进行过滤，不用将流量流入抗D设备，从而使防御与反射放大类压制更有效果。

### 2.3.4 流量预压制

流量预压制/UDP 预压制等能力，从容应对新型的超大流量攻击 （Memcached的5W 倍反射）。

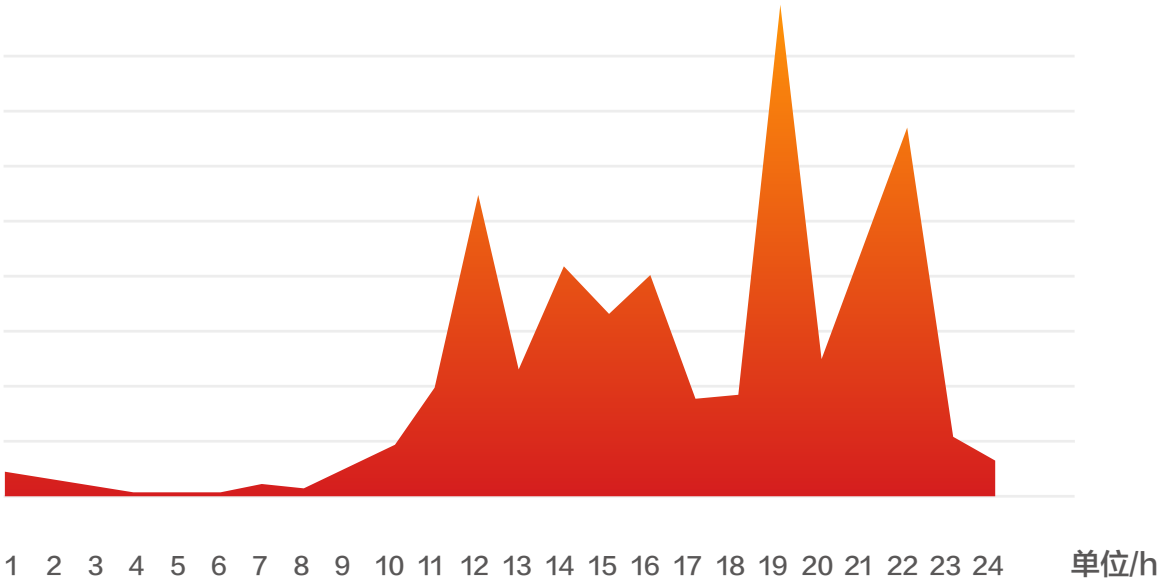
### 2.3.5 基于区块链技术 DDoS 固证

在 DDoS 防御产品及后台平台底层架构上利用区块链上数据不可篡改和可溯源的特性，将电子存证数据按照时间的顺序放到区块链中，以此提高数据的可信度，确保数据无法被更改，增加集成固证取证能力，为被攻击的用户提供出证服务，协助溯源。

# 第三章 2018年DDoS攻击情况

## 3.1 DDoS 攻击发生时间段

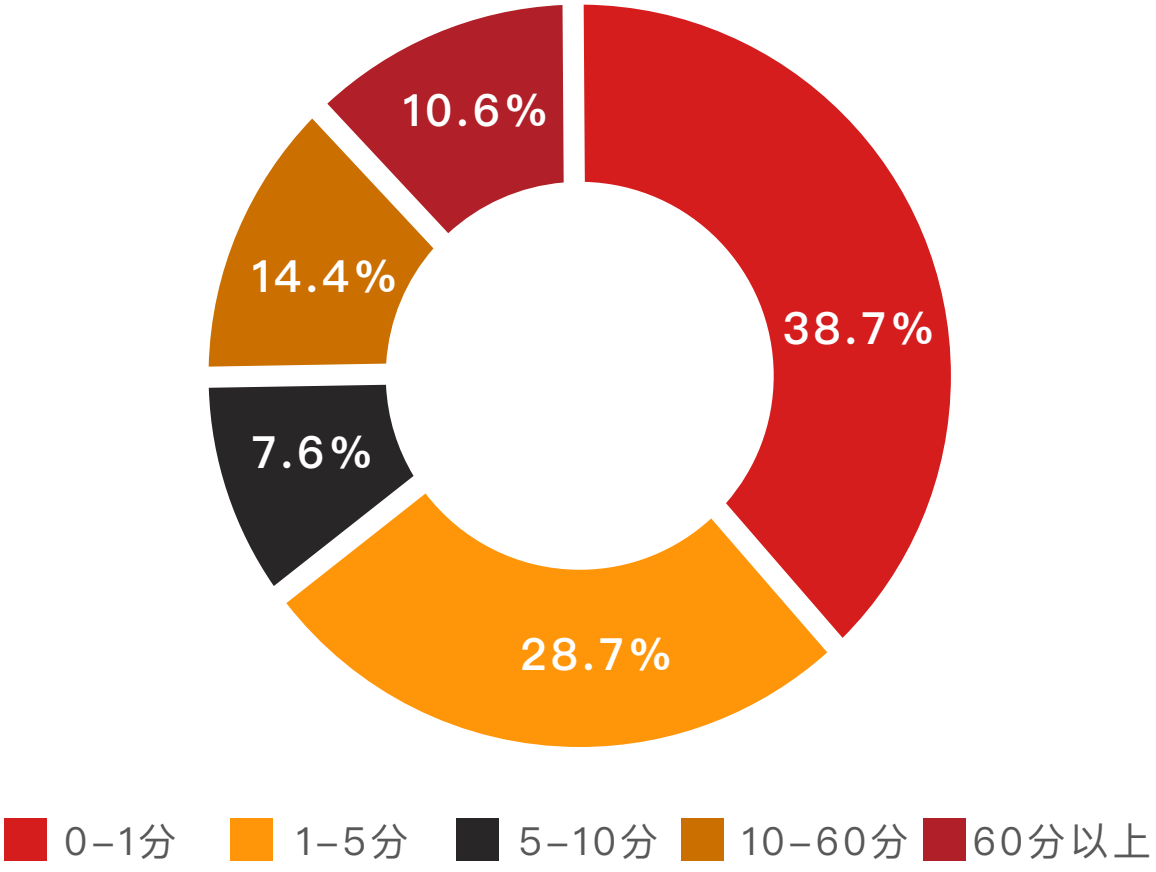
DDoS 攻击时段多为业务高峰期或在线人数最多时段，以达到最大的破坏效果。国内抽样 DDoS 数据可知，DDoS 的高峰期以上午10点到晚上23点为主，其中18点左右有一个低谷，但相比上午10点前仍高出很多。




DDos 攻击发生时间段统计

## 3.2 DDoS 攻击持续时间

随着 DDoS 的自动平台化，攻击时长越来越短，主要是归结于较好的平台有稳定的流量输出，使整体攻击时间控制在5分钟以内，期中38.7%集中在1分钟以内。相对而言，超过60分的攻击一般流量不大，且主要为 HTTP Flood、SYN Flood 小包等消耗资源类攻击。

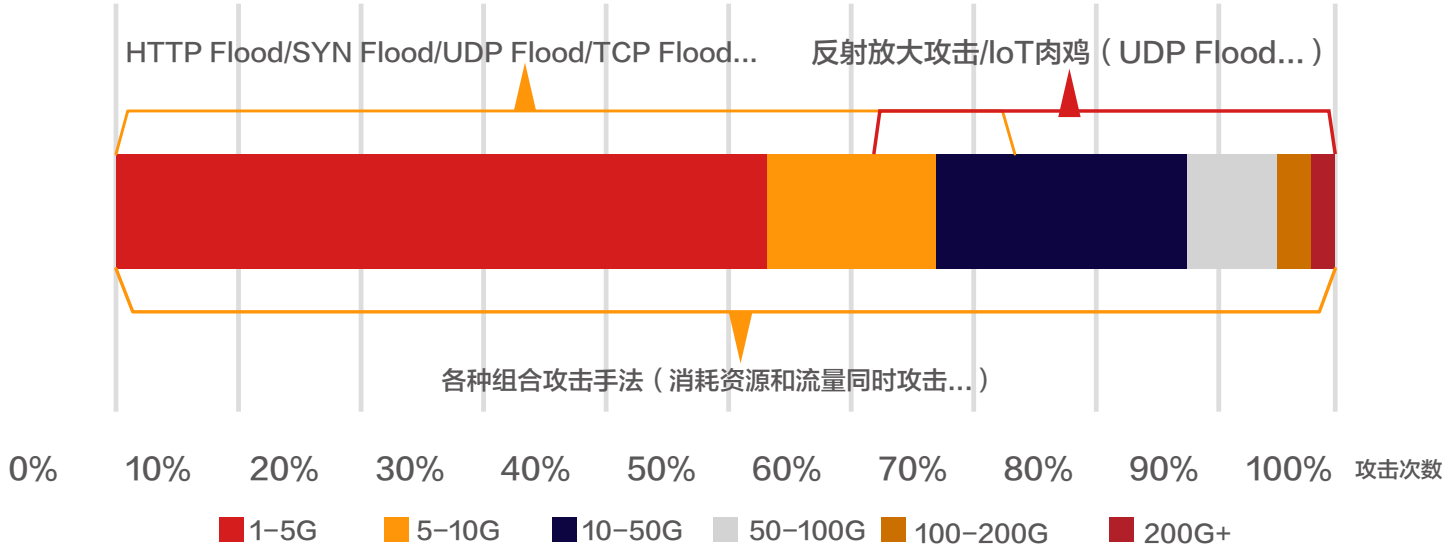



DDoS 攻击持续时间占比统计

## 3.3 攻击类型各流量区间分布

按攻击次数统计，主要的攻击流量区间在 5G 以内，其占比超过一半以上。但在流量区间占比分布基础上进行攻击类型的对应分类，则比较难以区分，存在很多交叉现象。

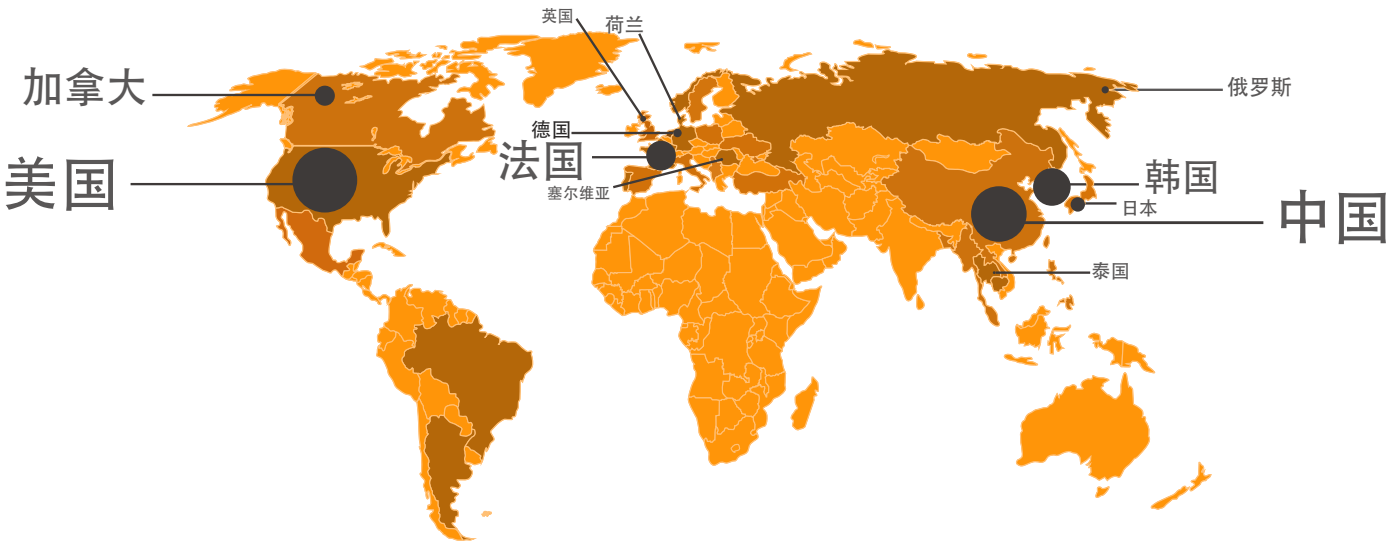
例如 IoT 肉鸡以 UDP Flood 或 SYN Flood 大包等攻击类型也可以打出百 G 流量，而目前百 G 流量主要还是以反射放大的形式打出流量，另在 10G 到 100G 之间，攻击类型交叉也很明显。值得一提的是现在越来越多的 DDoS 攻击，会进行组合攻击，使防御难上加难，达到最大攻击效果。




攻击类型各流量区间分布统计

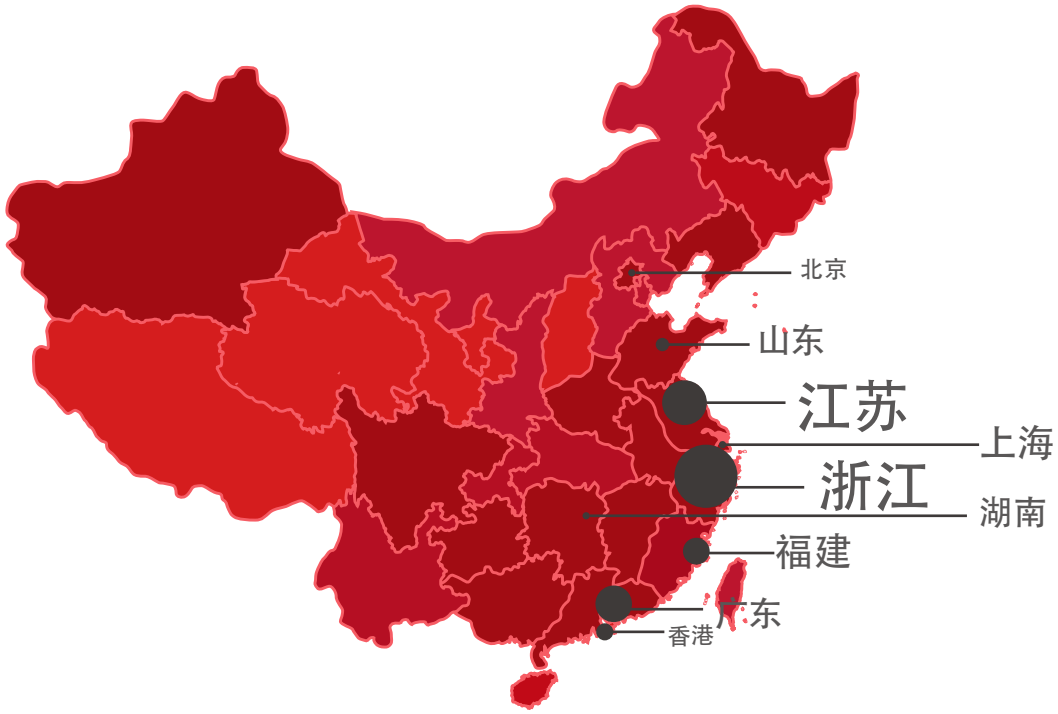
## 3.4 全球 DDoS 攻击目标国家占比

国外被 DDoS 攻击的国家涵盖很广，基本互联网覆盖到的地方，都有 DDoS 的身影。那些互联网大国更是首当其冲，例如美国、韩国以及西欧诸国。DDoS 的目的无非获利，所以竞品攻击与 DDoS 勒索占主要地位，国外这些发达的互联网国家在获利上更加便捷，所以受到的攻击占比也更大。



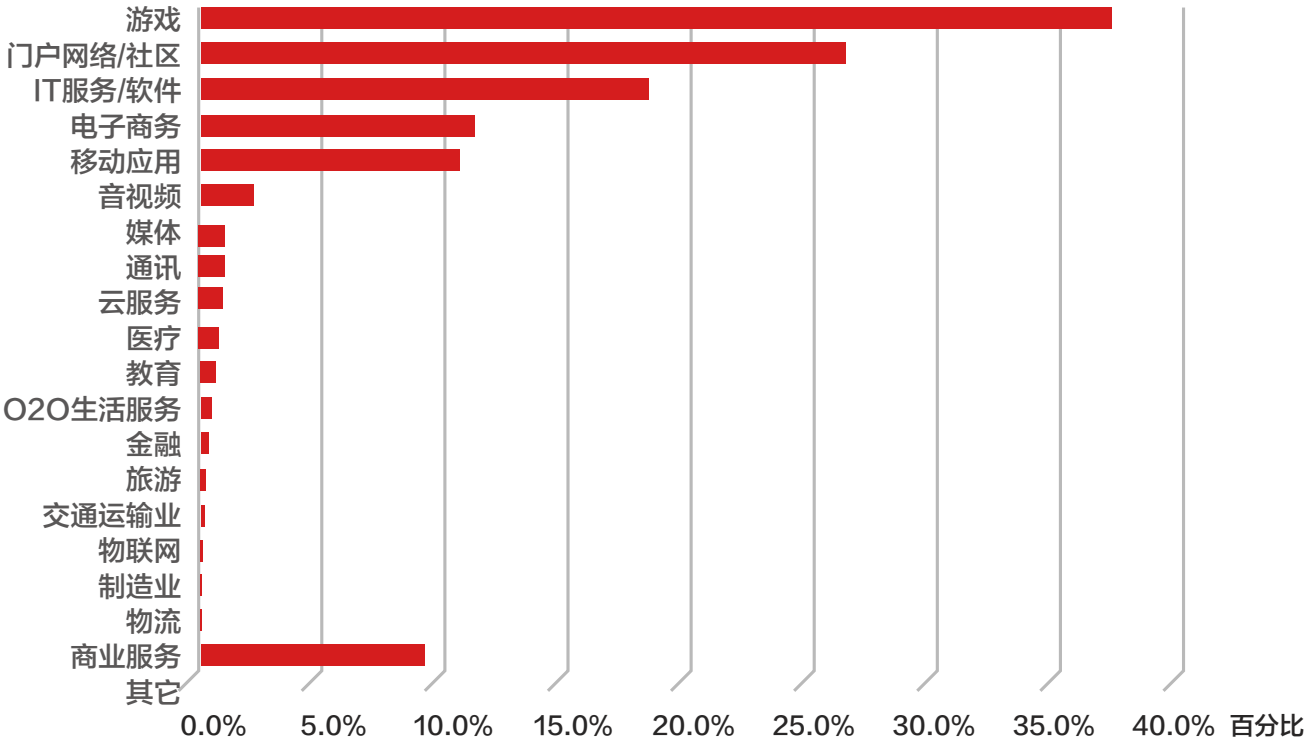
## 3.5 中国 DDoS 攻击目标各省份占比

国内被攻击的区域与国外情况类似，也多发于互联网建设较好的地区，如江浙、北京、香港。与历年攻击目标省份占比进行对比，各省占比均无甚变化，因为互联网的基础设施要花费大量时间进行建设，周期较长，且互联网程度越高的城市，网络的升级换代越快，对应的各种业务互联网化转化也越便捷，因此 DDoS 可能会攻击的业务线也越多。



## 3.6 攻击目标行业分布

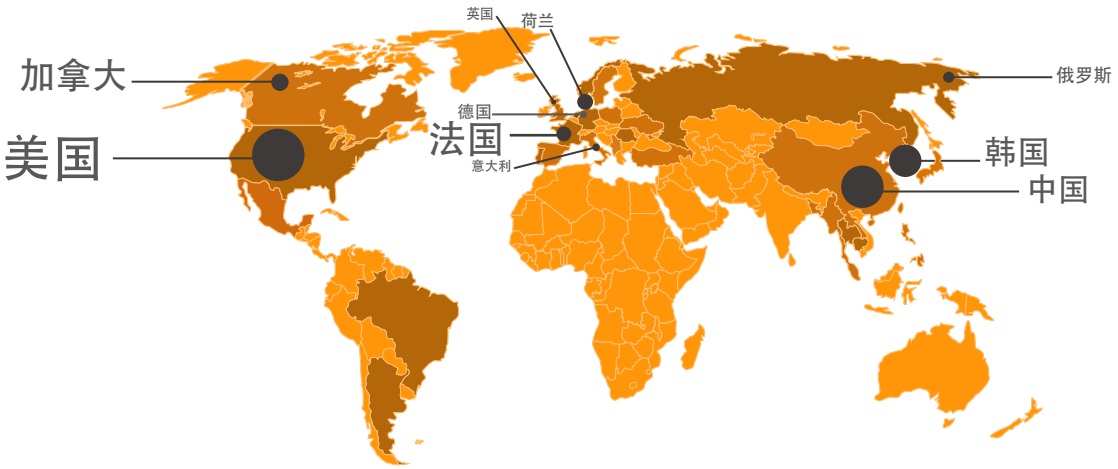
攻击目标的行业众多，可以说只要互联网化的行业，都有被涉及到，其中以游戏行业为最。在游戏之外，新兴的音、视频有上升的趋势，和当今流行的直播、短视频等有关。另外在医疗、制造业、物联网等行业中 DDoS 也崭露头角，可见利益总是最好的攻击导向。




DDos 攻击目标行业分布占比统计

## 3.7 僵尸网络 C2 服务器全球分布

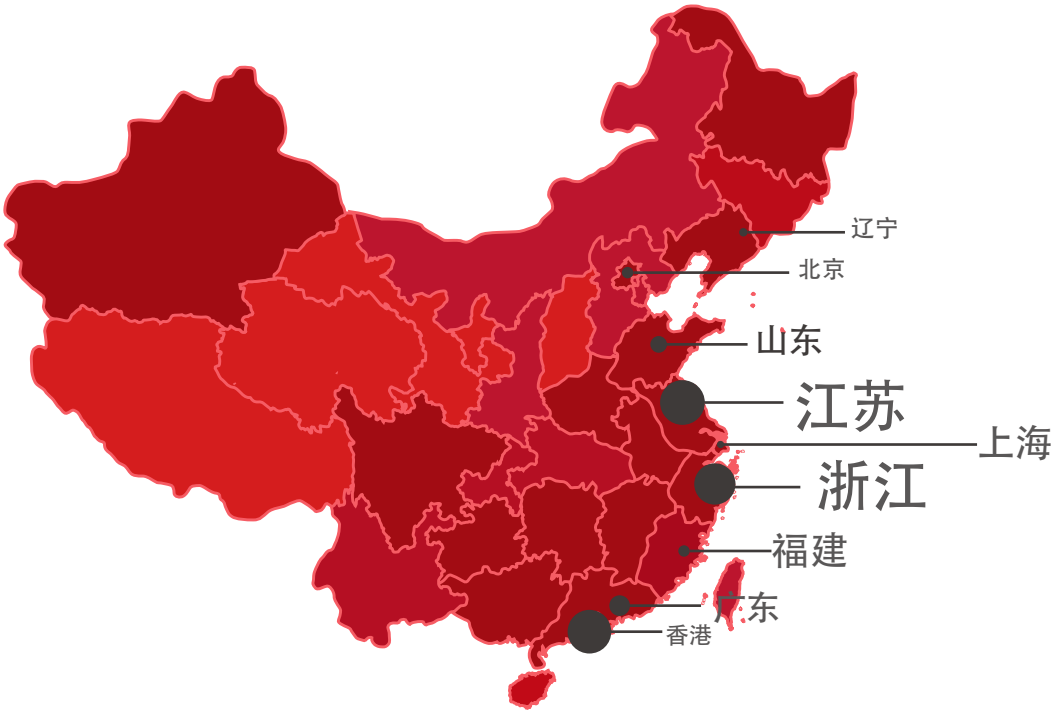
提起僵尸网络，那么大家最关心的无外乎便是 C2 信息或反射放大的发包机位置信息等。C2 服务器在全球分布，主要以中国、韩国、美国、欧洲国家为主，随着中国打击 DDoS 力度越来越大，C2 有外迁到第三方世界的小国家，这些国家网络监控宽松，能躲过监查，且针对流量上可以有伪造源 IP 的各种攻击输出，这也是发包机为什么大多在国外的原因。




僵尸网络C2服务器全球分布统计

## 3.8 僵尸网络 C2 服务器国内分布

僵尸网络的 C2 在国内情况，与前文分析的类似，主要集中在互联网建设较好的省份，香港作为一个网络管理相对宽松的区域，存在好多的业务线互联网化，所以占比排名第二。国内的僵尸网络打击力度越来越大，导致 DDoS 的好多 C2 迁移到国外。




僵尸网络C2服务器国内分布

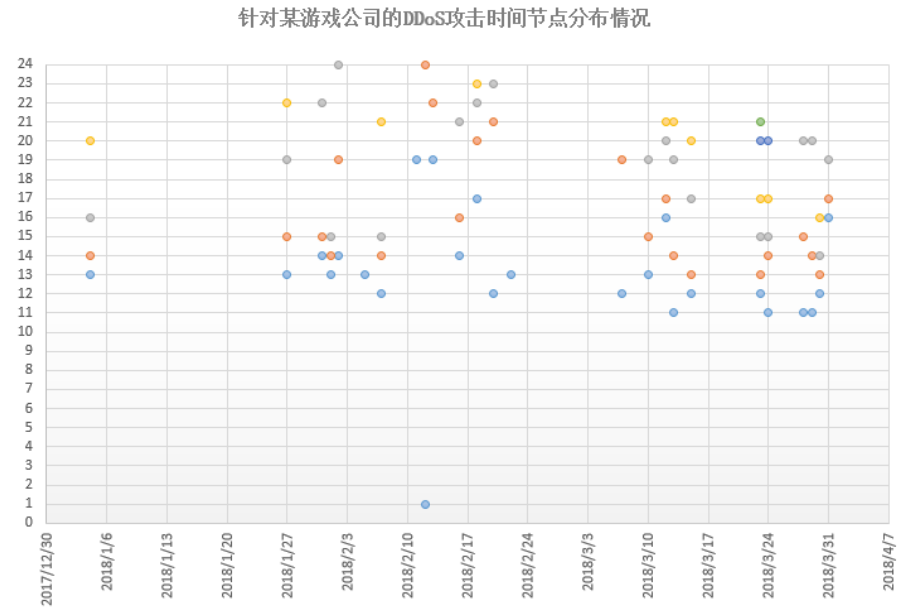
## 3.9 典型攻击事例

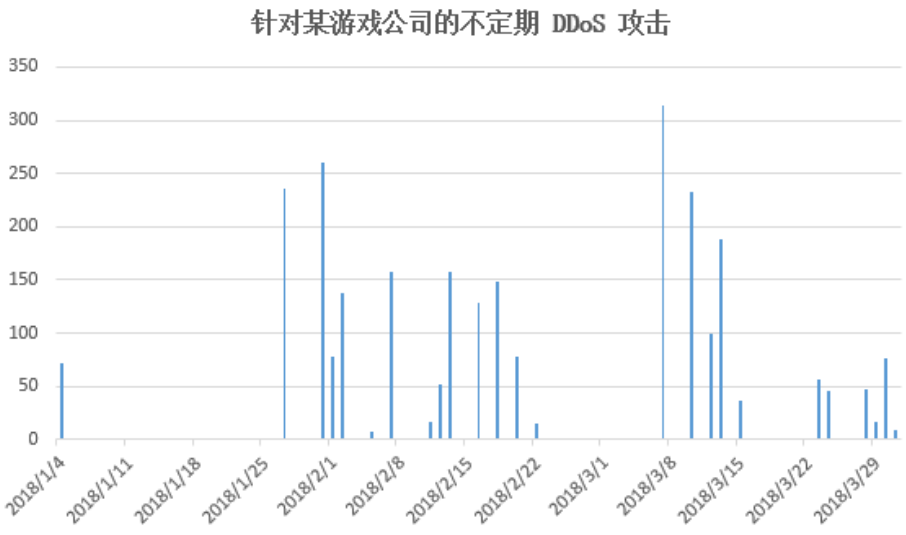
下面以2018年第一季度针对腾讯云某游戏公司的 DDoS 攻击为例，进行典型攻击方法的分析。此 DDoS 案例特点是发起攻击持续时间长，且攻击范围逐渐扩大。下表是被攻击 IP 与日期的映射关系，在三个月中受到持续攻击中，被攻击 IP 数量多达18个，其中1月与2月攻击 IP 单一，3月份后被攻击 IP 持续增多。其中1月4号的一个单 IP 攻击便达到了上百 Gbps 的流量。

| IP \ date | 1/04 | 1/27 | 1/31 | 2/01 | 2/02 | 2/05 | 2/07 | 2/11 | 2/12 | 2/13 | 2/16 | 2/18 | 2/20 | 2/22 | 3/07 | 3/10 | 3/12 | 3/13 | 3/15 | 3/23 | 3/24 | 3/28 | 3/29 | 3/30 | 3/31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 119.*.*.93 | * | * | | | | | | * | * | * | * | | * | | | | | | * | * | * | | | | |
| 123.*.*.168 | * | | | | | | | | | | | * | | | | | | | | | | | | | |
| 123.*.*.16 | | * | * | * | * | * | * | | | | | | | | | * | * | | | | | | | | |
| 118.*.*.167 | | | | | | | | | | | | | * | | | | | | | | | * | | | |
| 118.*.*.49 | | | | | | | | | | | | | * | * | | | | | | | | * | | | |
| 123.*.*.78 | | | | | | | | | | | | | | | * | * | * | * | * | * | * | * | | | |
| 123.*.*.123 | | | | | | | | | | | | | | | * | * | * | * | * | * | * | | | | |
| 119.*.*.200 | | | | | | | | | | | | | | | | * | * | | * | * | * | * | | | |
| 139.*.*.64 | | | | | | | | | | | | | | | | | * | * | * | * | * | | | | |
| 123.*.*.207 | | | | | | | | | | | | | | | | | | * | * | * | * | | | | |
| 111.*.109.* | | | | | | | | | | | | | | | | | | | | * | | | | | |
| 123.*.*.249 | | | | | | | | | | | | | | | | | | | | * | | | | | |
| 111.*.*.111 | | | | | | | | | | | | | | | | | | | | | | * | | | |
| 111.*.245.* | | | | | | | | | | | | | | | | | | | | | | * | | | |
| 111.*.*.15 | | | | | | | | | | | | | | | | | | | | | | * | * | * | * |
| 111.*.*.177 | | | | | | | | | | | | | | | | | | | | | | | | * | * |
| 119.*.*.149 | | | | | | | | | | | | | | | | | | | | | | | | * | * |
| 139.*.*.32 | | | | | | | | | | | | | | | | | | | | | | | | * | |

| 序号 | 被攻击 IP | 被攻击次数 |
|---|---|---|
| 01 | 123.*.*.16 | 769 |
| 02 | 119.*.*.93 | 592 |
| 03 | 123.*.*.123 | 416 |
| 04 | 123.*.*.78 | 242 |
| 05 | 123.*.*.168 | 207 |
| 06 | 123.*.*.207 | 107 |
| 07 | 119.*.*.200 | 95 |
| 08 | 118.*.*.49 | 62 |
| 09 | 111.*.*.15 | 49 |
| 10 | 139.*.*.64 | 38 |
| 11 | 139.*.*.32 | 33 |
| 12 | 111.*.*.177 | 16 |
| 13 | 118.*.*.167 | 15 |
| 14 | 119.*.*.149 | 13 |
| 15 | 111.*.*.111 | 4 |
| 16 | 111.*.*.147 | 3 |
| 17 | 123.*.*.249 | 2 |
| 18 | 111.*.245.* | 2 |

攻击发起日期与攻击时段与上文中分析的一致，均是在游戏上线高峰期进行攻击。



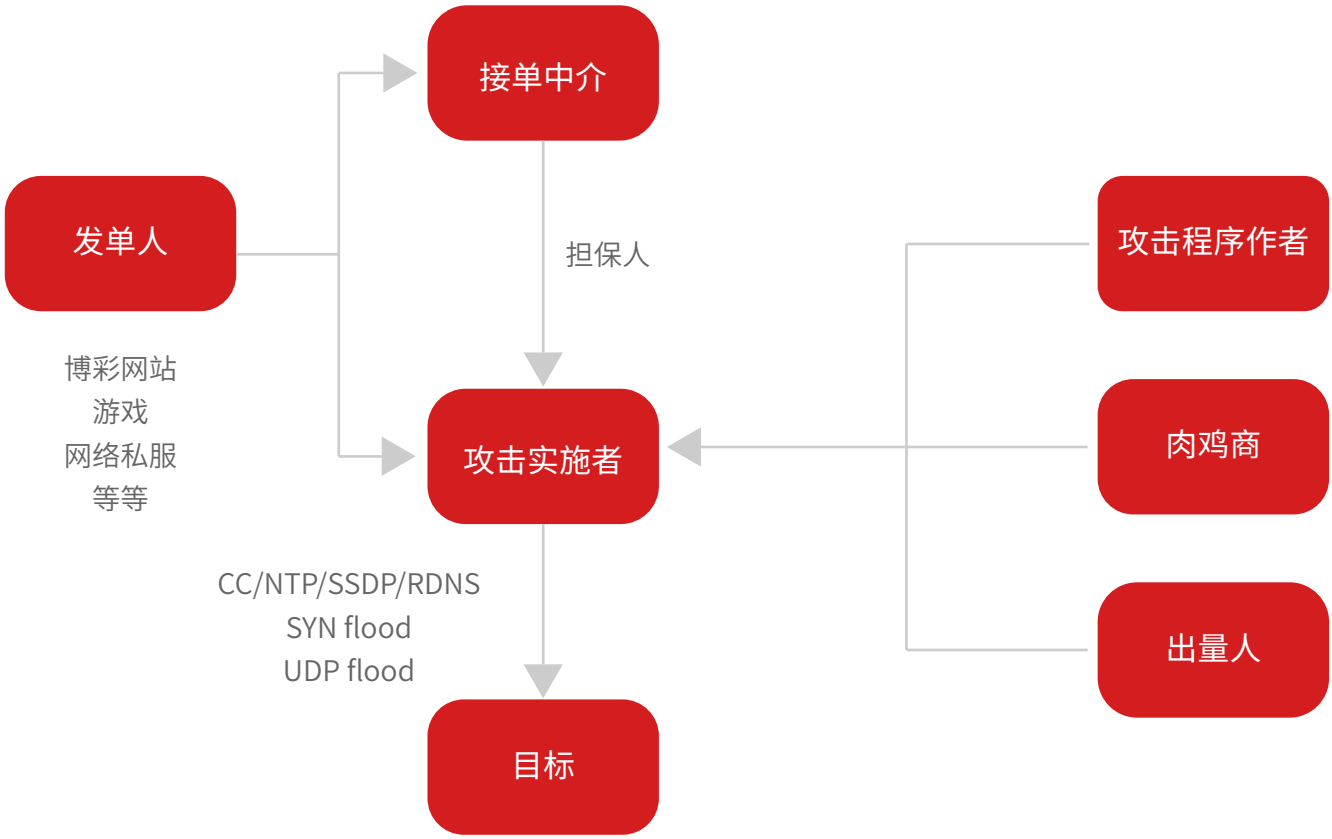




针对此公司的 DDoS 攻击由7个僵尸网络不定期的发起攻击，每个僵尸网络均发起过上百次的攻击，攻击方法主要是带有 payload 的 SYN Flood 攻击，以持续消耗带宽，导致游戏掉线或网络堵塞。在针对攻击细节的分析中发现，这7个不同的僵尸网络会有多个在同一时段同时发起针对同一 IP 的攻击的情况，而且攻击的数据包相似，所以将这几个僵尸网络可以暂时归结到一个黑客组织控制与管理，方便后续的防御与溯源。

# 第四章 DDoS 产业链及新变化

## 4.1 DDoS 产业链

DDoS 攻击犯罪已经进入产业化时代——从以往的需要专业黑客实施全部攻击过程的行为，发展成由发单人、攻击实施人、肉鸡商、出量人、黑客攻击软件作者、担保人等多个犯罪个体共同参与实施的产业化犯罪行为。



### 4.1.1 发单人

一次 DDoS 攻击往往始于发单人，DDoS 攻击的发单人来自各行各业，同行竞争是 DDoS 的主要原因之一。因此，发单人与受害者往往身处同一行业。

最为典型的发单群体就是博彩网站站长。2016年6月14日，一家中国博彩公司不幸遭遇多矢量 DDoS 攻击，攻击者以 470 Gbps 和超过 110 Mpps 对其服务器实施猛攻。该公司在遭受攻击前几天已经遭到多个超过250+的攻击。攻击者利用9个不同的攻击矢量实施攻击。博彩网站往往利用 DDoS 攻击，使得竞争对手无法正常开展业务，从而争夺用户资源。

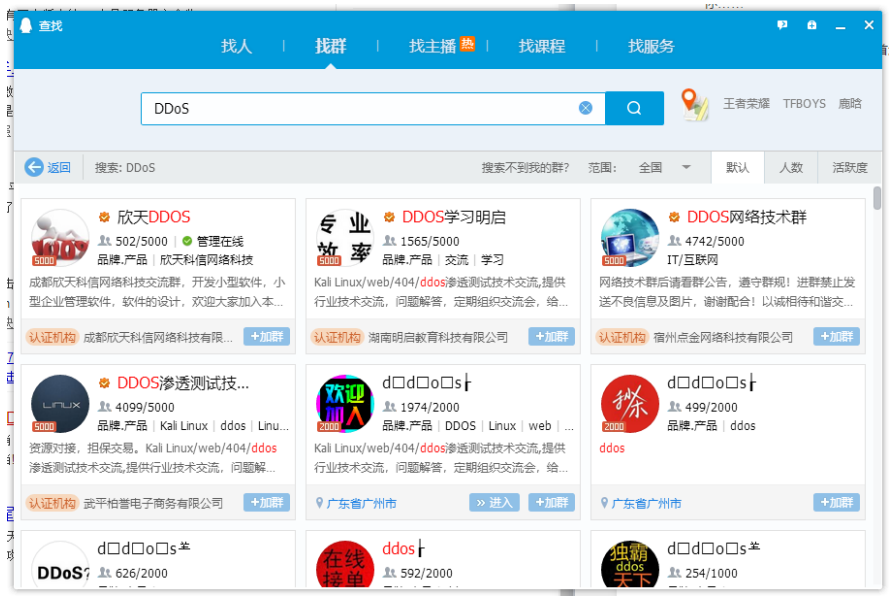
同样需要争夺用户的还有游戏行业，特别是网游私服。由于其背后的高收益，使得游戏行业成为了发单群体中必不可少的一个部分。在我们针对目标行业的统计中，游戏行业的攻击占比高达35%以上，其中大部分的攻击也都来源自同行竞争。

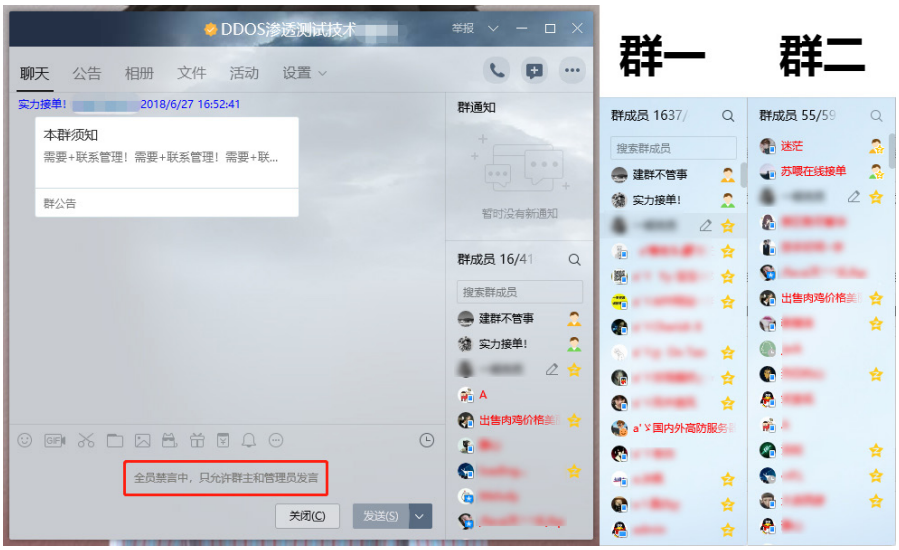
### 4.1.2 发单渠道

和其他黑产行为一样，想要寻找 DDoS 服务提供方，完全不必大费周章的上暗网、Telegram 群里去进行沟通、交易。通过 QQ、淘宝、百度贴吧等渠道可以很轻松地找到提供 DDoS 的服务商，甚至可以等他们自动找上门……

### 4.1.3 QQ渠道

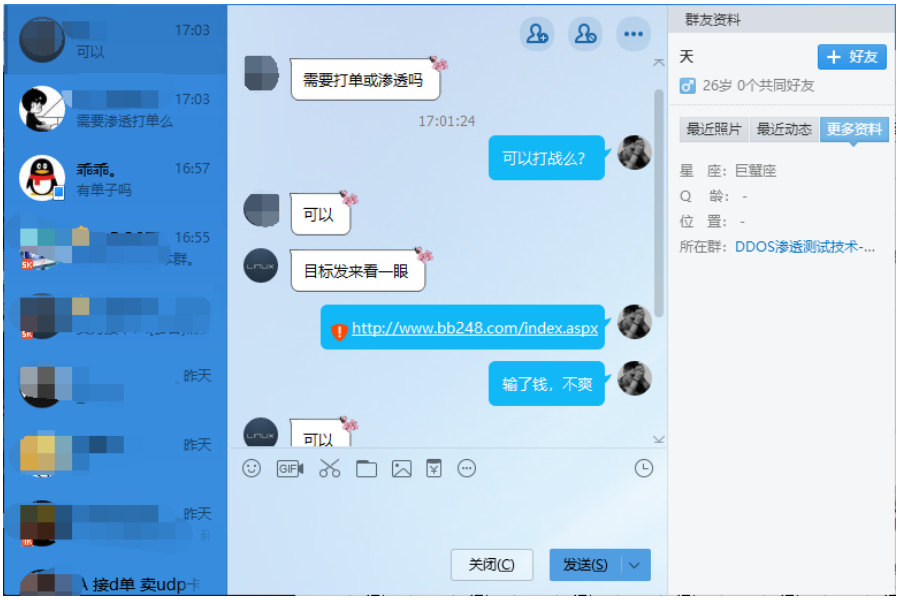
在这几个渠道里，QQ 一定是首选。首先在 QQ 群查找页直接搜索“DDoS”，就会出来大量的 QQ 群，群成员人数4000+的不在少数。部分群在群名称以及介绍中明确表示是技术交流群，更多的则是能够明显看出来是提供 DDoS 攻击服务的。




绝大部分 DDoS 群都是设置“全员禁言状态，只允许群主和管理员发言”，那么这种群存在的唯一意义就是提供服务方与需求方的对接，通过私聊即可直接联系。

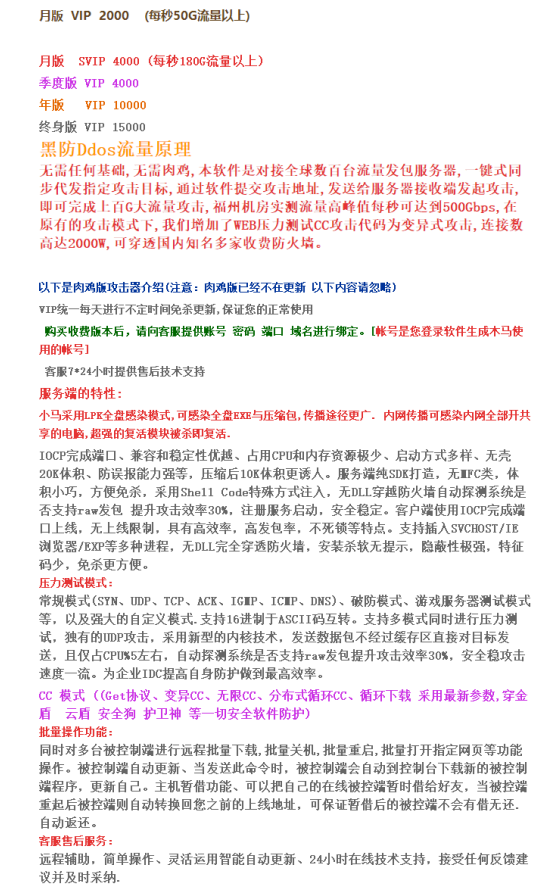
进群之后，立刻有很多人发送私信以及加好友申请。可见一旦这个圈子里出现新人，产业链背后的从业者就会如猛虎扑食，一拥而上。


需要打单或渗透吗
17:01:24
可以打战么?
可以
目标发来看一眼
http://www.bb248.com/index.aspx
输了钱，不爽
可以
关闭(C)
发送(S)
群友资料
天
好友
26岁 0个共同好友
最近照片
最近动态
更多资料
星 座：巨蟹座
年 龄：-
位 置：-
所在群：DDOS渗透测试技术-...


验证消息
好友验证
群系统消息
今天
来自QQ群 - DDOS渗透测试技...
女 27岁
附加消息：我是黑色产业链接 回复
同意
忽略
zhangqiang 来自临时会话
- - 东莞
附加消息：申请加我为好友 回复
同意
忽略


ddos
聊天
公告
相册
文件
活动
设置
【潜水】行走的荷尔蒙(3392260563) 2018/6/27 14:58:53
DDOS攻击 价位最低多少?
打普通服务器
【管理员】苏喂在线接单(27666273) 2018/6/27 15:00:22
1
【潜水】行走的荷尔蒙(3392260563) 2018/6/27 15:05:02
有网站吗？？我要购买攻击
价格低的联系我
【管理员】苏喂在线接单(27666273) 17:40:58
富强、民主、文明、和谐.
自由、平等、公正、法治.
爱国、敬业、诚信、友善.
群通知
群成员 56/59
苏喂在线接单
关闭(C)
发送(S)


一个卖家表示，一个月的时间就能够打垮目标网站，收费3000元。另一家则表示300元就可以搞定，并自称“到死也查不到（谁干的）”。




暗访期间，还能找到一些提供 DDoS 服务的网站，可以直接下载对方所提供的软件，通过购买天卡、月卡或者年卡使用。不同点卡在价格上可能存在较大的区别，但相同之处在于，所有点卡交易都是通过第三方发卡平台进行，也许是为了有效隐藏收款渠道。

### 4.1.4 淘宝渠道

除了 QQ 之外，万能的淘宝再次发挥了它的神奇作用。DDoS 攻击之类的字眼也在淘宝上疑似被封禁，但仍有大量提供 DDoS 防护的店铺。通过旺旺联系多个卖家，询问是否提供压力 测、DDoS 攻击等服务，最终能获取一些结果。


询问卖家是否提供 DDoS 服务，如果卖家答案是确定的，那么他就会告知需求方通过 QQ 联系，接下来的步骤便与 QQ 渠道部分内容相同。

### 4.1.5 搜索引擎

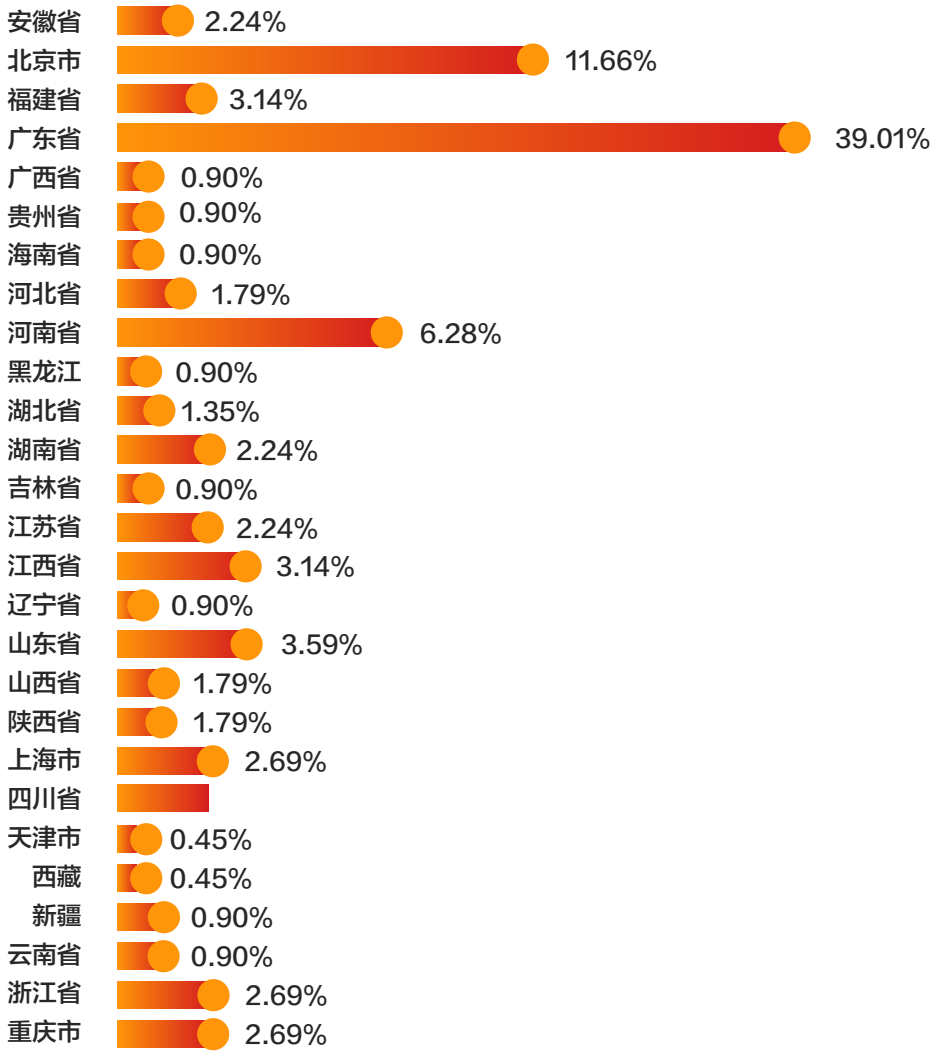
通过在 QQ、淘宝等渠道暗访调查，可轻易获取有效的 DDoS 服务交易关键词，如天罚“DDoS”、“大金 DDoS”等。这些大多是一些 DDoS 攻击的执行软件，在搜索引擎搜索这些关键词，能够很快找到大量相关的平台网站。



虽然不少平台表面上看起来是正规的压力测试服务，但却打出了疑似黑产擦边球的标语，不论是“代天执法”还是“替天行道”，都有浓厚的江湖气息。

此外，在带有“DDoS”关键字的贴吧以及一些黑客论坛里，找到提供 DDoS 服务的人都毫不费力。找到相关人员后，都可通过 QQ 或者微信进一步联系。总而言之，在国内，想要找到 DDoS 攻击服务的提供商完全不需要折腾去暗网，毕竟压力测试和 DDoS 服务之间也只在一念之差。

## QQ 群地域分布




通过关键词“DDoS”、“渗透测试”、“压力测试”等查询 QQ 群，粗略统计其所在地域分布情况，以广东、深圳、北京为主，其次上海、浙江、四川等其他地方均有些许分布。

群人数规模

报告统计了总共188个 DDoS 相关的讨论群，其中有4个 QQ 群的人数规模达到了5000人，而且基本满员。而2000人群、1000人群分别达到了28个、15个。通过这些能够初步估计通过 QQ 群完成潜在 DDoS 攻击交易及 DDoS 服务传播的规模。

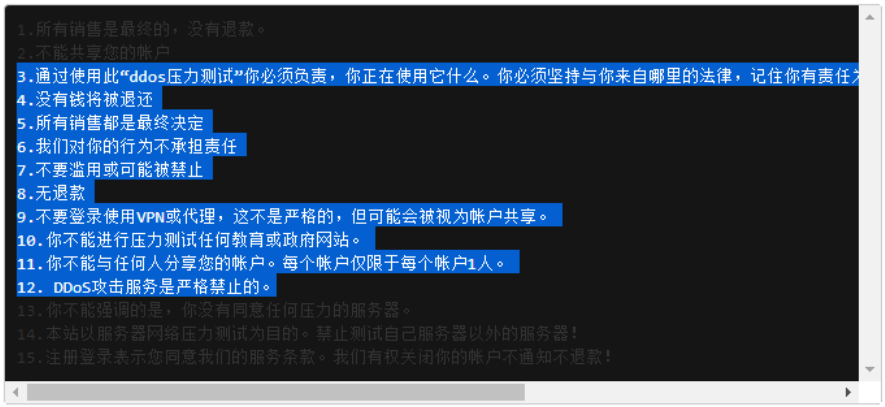
### 4.1.6 接单中介

DDoS 黑产的高度成熟也催生出产业链条中的中介服务：接单中介。最基础的模式是接单人员接到客户的基于不同需求的“D 单”、“C 单”、“包天单”等订单，再把单子分发给具备相应攻击资源和能力的攻击者。根据对目前黑市的调查，完成一份 D 单的报酬根据攻击难度和攻击时长从100元到上千元不等，接单中介按协商好的百分比收取利润。

也有的接单中介本身拥有较小的流量，如果需求较小，可以自己完成攻击，当需求较大时再转给专门的攻击手。
不过随着页端 DDoS 攻击平台的兴起，接单中介这种中间人角色已经逐渐被取代。如此一来，既精简了交易环节，也方便购买者直接通过页端平台自主操作。

### 4.1.7 攻击程序

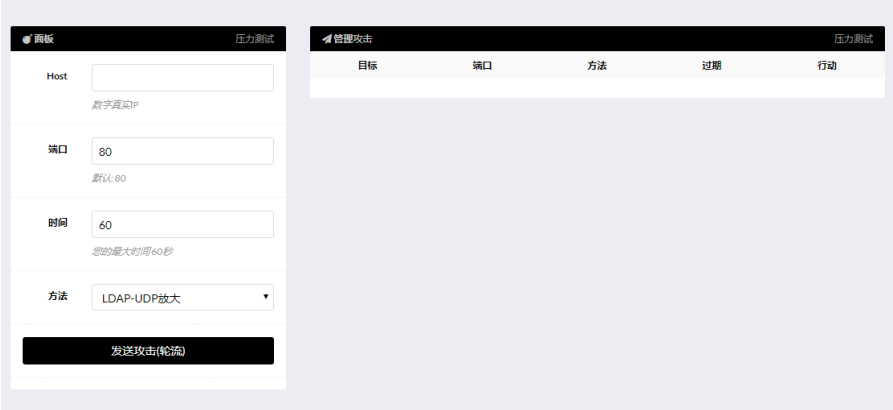
从 QQ 群等渠道接触到各种 DDoS 服务提供商，虽然现在仍然有提供软件端服务的商家，但更多的还是在网页端，基本上每一个人数较多的 DDoS 服务群都对应一个页端平台。压力测试和 DDoS 攻击处于黑与白之间，界限太模糊。所以压力测试这这类服务的网页过审、正常运营并没有什么问题，也正因为这样 DDoS 黑产又多了一层外衣。

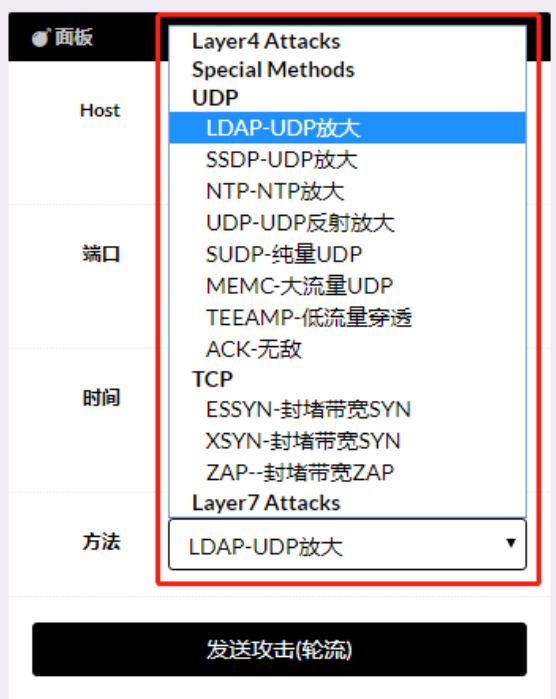



从以上提到的 DDoS 平台中挑出一家注册账户探究，在用户协议中明确提到“DDoS 攻击服务是严格禁止的”、“使用 DDoS 压力测试你必须对自己的行为负责”等。

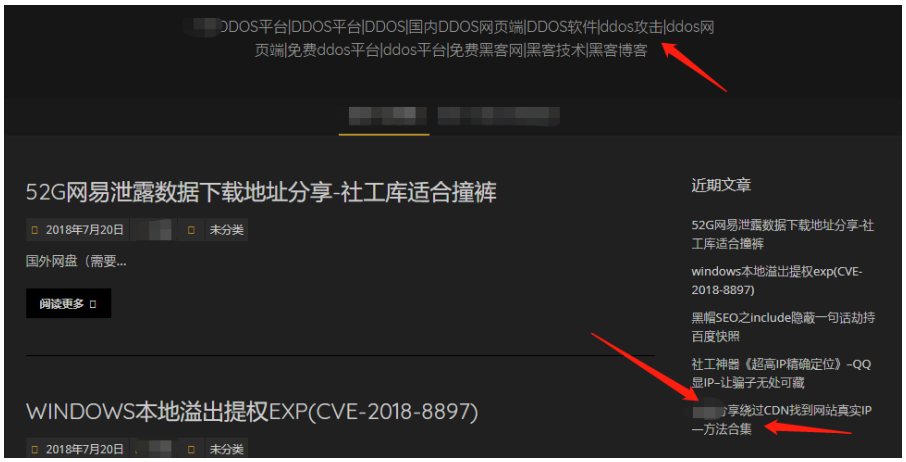

不过这些网站在搜索引擎中结果展示都带有“DDoS 攻击”的字样，整个注册过程中并不需要实名认证、绑定手机号等，只需要一个邮箱即可，如果被黑产利用进行非法攻击，基本无迹可寻，而IP地址也可以伪造。


进入平台后台，可以看到该平台发起的总攻击数量以及注册用户数量（该平台声明会定期删除未购买套餐或者套餐过期的用户）。



必须购买套餐激活后才能进入该平台的压力测试区，只需要填写目标站点的 Host、端口、时间即可发送攻击，攻击方法也有多种可选，至少在这个环节，压力测试和 DDoS 攻击是没有区别的，就看使用者的目的了。




有意思的是，该平台有站长个人微博的外链，能够看“DDoS 攻击”字眼，还有一篇《绕过 CDN 找到网站真实 IP》的教程文章，这很难不让人与黑产联系到一起。

这一类页端 DDoS 攻击平台在搜索引擎中比比皆是，后台布局高度相似。虽然仅凭这些调查不能判定某个平台是否从事黑产，但这些平台绝对是黑产最可能利用的渠道之一。

### 4.1.8 流量平台

一般采用国外的 IDC 机房租用 G 口带宽服务器做为发包机，进行反射放大攻击、SYN Flood 攻击。因为国外一些 IDC 机房监管不严，可以非本机房伪造源 IP 的数据包在网络在传输，这给 DDoS 的攻击创造了很大的便利，同时给防御带来了新的挑战。

CC 攻击流量，采用传统肉鸡形式，因其要建立 TCP 的长连接，所以伪造源IP就不可行了，必须要大量肉鸡做这真实的出口来进行 CC 攻击。同理 TCP Flood 也是如此。

IoT 类的 botnet 在整体的流量上占有很大的比例，因为 IoT 类设备无安全防护，且有一些账号密码是出厂固化，比弱口令更不安全。IoT 类的 botnet 在 bot 端以弱口令或产品漏洞自传播模式为主，在控制端主要以 API 的模式发起攻击指令。在发起攻击指令处已有成熟的自动化调度策略，可以与页端 DDoS 攻击平台无缝衔接。

页端 DDoS 攻击平台是目前 DDoS 的最成熟的攻击平台，会以各种隐蔽手段存在。例如“压力测试平台”、“攻击演练平台”等，还有一些甚至直接叫 DDoS 攻击平台，在暗网上多以 DDoS 攻击平台直接标示。页端 DDoS 攻击平台已日渐代替 DDoS 中间人的角色，是 DDoS 发起攻击的主要入口。其后端可管理调度发包机、带自动 API 的 botnet 等。

### 4.1.9 攻击实施

目前主流的 DDoS 攻击手段可参考本文第二章，黑客攻击者也被自动化攻击平台所取代。从发起攻击命令到真正开始攻击，延时降低到了 10s 的水平，攻击效率大大提高。页端 DDoS 攻击平台往往会伪装成“流量压力测试平台”，并由站长进行平台的综合管理、部署、运维工作。

## 4.2 产业新变化

### 4.2.1 暗网 DDoS

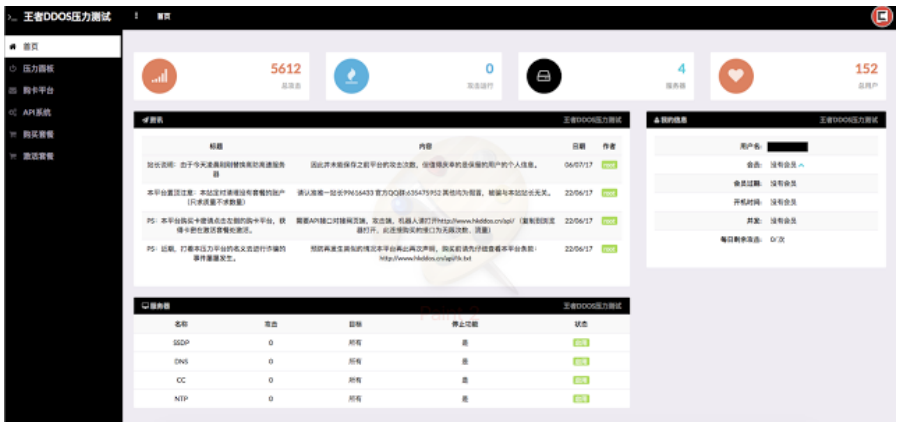
美国云安全技术服务公司 Armor 近期发布的一份报告，揭示了暗网上针对各种网络犯罪相关服务实施的价格标准。

根据 Armor 的说法，用户可以以10美元/小时、200美元/天的价格或者500美元/12000美元的价格租用 DDoS 攻击。银行僵尸网络（750美元/月），漏洞利用套件（1400美元/月），WordPress 漏洞（100美元），ATM 分离器（1,500美元）和黑客入门教程（50美元）也可以出售。

| HACKING TOOLS & SERVICES | |
|---|---|
| Account Hacking Program | **$12.99** (See more details on page 10) |
| Hacked Instagram Accounts in Bulk | 1,000 - 10,000 accounts **$15 - $60** |
| Botnet: Blow-Bot Banking Botnet | Monthly Basic Rental **$750** I Monthly Full Rental **$1,200** I Monthly Support **$150** |
| Disdain Exploit Kit | Day **$80**, Week **$500**, Month **$1,400** |
| Stegano Exploit Kit: Chrome , FireFox, Internet Explorer, Opera, Edge | Unlimited Traffic, Day **$2,000** Unlimited Traffic, Month **$15,000** |
| Microsoft Office Exploit Builder | Lite exploit builder **$650** Full Version **$1,000** |
| WordPress Exploit | **$100** |
| Password Stealer | **$50** |
| Android Malware Loader | **$1,500** |
| Western Union Hacking Bug For World Wide Transfer | **$300** |
| DDoS Attacks | Week long attack **$500 - $1,200** |
| ATM Skimmers: Wincor, Slimm, NCR, Diebold | **$700 - $1,500** |
| Hacking Tutorials | Multiple Tutorials **$5 - $50** |

全球比较大的暗网平台一般都会出售 DDOS 服务、DDOS API 接口、僵尸网络等。与此同时，在暗网的地下论坛也有大量售卖 DDoS 攻击工具的渠道。根据卡巴斯基的调查，暗网的 DDoS 商户可以获取到95%的盈利空间。由于暗网的隐蔽性，提供服务的商户可以将 DDoS 这样违法的服务以看似非常正规的服务方式推出，他们会提供基于 Web 的界面，与那些网上商城类似。客户可以查询到余额、配置等信息。

### 4.2.2 DDoS as a Service




DDos as a Service 商户提供的服务往往取决于最大攻击持续时间和所需的并发攻击数量，这个价格通常从10美元至200美元不等。

有很多提供服务的公司公开宣称业务是“压力测试”，然而在地下论坛中则将自己宣传为 DDoS 服务。

而一个新趋势是，DDos as a Service 这类的服务在中国地下市场越来越受欢迎。大量的在线 DDoS 服务网站使得 DDoS 服务更加定制化，也更加触手可及。

地下市场中存在大量的在线 DDoS 压力测试平台，这些平台很多使用了类似的界面，可以通过购买激活码发起攻击，并且客户可以使用一些参数来调节攻击。在某个 DDoS 平台的介绍页面甚至写道，其已经处理了来自44238名用户的168423个攻击请求。


对于这些 DDoS 平台，能够实施的 DDoS 攻击方式多种多样：

| 攻击名称 | 攻击层数 | 目标种类 | 命令填写格式 |
| --- | --- | --- | --- |
| GET | Layer 7 | 网站，服务器IP等 | 填写网站链接: http://xxxx.com |
| HEAD | Layer 7 | 网站，服务器IP等 | 填写网站链接: http://xxxx.com |
| POST | Layer 7 | 网站，服务器IP等 | 填写网站链接: http://xxxx.com |
| JSBYPASS | Layer 7 | 网站，服务器IP等 | 填写网站链接: http://xxxx.com |
| JOOMLA | Layer 7 | 网站，服务器IP等 | 填写网站链接: http://xxxx.com |
| XMLRPC | Layer 7 | 网站，服务器IP等 | 填写网站链接: http://xxxx.com |
| SNMP | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| SSDP | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| DNS | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| CHARGEN | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| NTP | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| TS3 | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| SSYN | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| DOMINATE | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| ACK | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| NGSSYN | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| OVX | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| TCPACK | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| TCPSYN | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| TCPRST | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| TCPURG | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| TCPPUSH | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| TCPECE | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| TCPCWR | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| ICMP | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| MUDP | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| VSE | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |
| ATCP | Layer 4 | 个人主机，服务器IP等 | 填写IP地址: 192.168.0.1 |

通过查看这些在线平台的源码可以发现，这些 DDoS 平台的网页端代码大多来自国外，经过汉化后在中国市场被广泛使用。除了语言的修改以外，一些中国特色的特性也被加入其中，例如支付方式往往会被修改为支付宝。

# 第五章 安全建议

《网络安全法》第十条规定，建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

建立网络安全防护体系，不仅是符合法律规定，更是为了保护网站和网民的安全。为此，企业应从多方面来部署完善的安全策略，具体建议如下：

1

在业务主机上要进行 IP 的过滤等设置，以应对同IP发起 DDoS 的情况。除常规的限次数、限地域外，还要以进行一些固定反射源的过滤，因为有反射源访问业务，一般都是不合理的，这样有助于快速排查问题所在，及时开启防护。

2

隐藏真实的业务 IP ，进行 IP 保障，以让攻击者攻击时增加定位难度。

3

针对业务，要进行多份保障及 CDN 使用，分散攻击面，使攻击者的整体攻击成本加大，也是一种变相防御手法。

4

针对业务的侧重点不同，要选择有针对性的 DDoS 防护产品。不用大而全，过度浪费，也不能不设置防御，被攻击时临时抱佛脚。

5

及时进行服务器中的系统及各应用软件的补丁更新，随时关注安全时势动态，针对一些 0day 或未能及时修复或处理的逻辑漏洞进行人工的临时策略处理。这样可以防止服务器被入键或被用作反射点，Memcached 反射源就是最好的例子。被用作反射源会对外发出大量的数据包，会占用自身海量的带宽，也是一种变相的遭受 DDoS 攻击的受害者。

6

在业务代码侧与逻辑侧，做好 DDoS 攻击的类型的预防，例如针对 SYN Flood 这种半开连接，可以在业务展前端做一层代理层，来吞吐流量，将 TCP 成功连接后的再去唤醒业务侧真正的服务处置等。

除此之外，在第四章的分析中，我们发现大量 QQ 群、微信群以及淘宝店已成为 DDoS 黑色产业链的重要组成部分，部分群主甚至是在读大学生，个中现象引人深思。相信通过监管单位的进一步加强监管、充分引导，推动更多网络安全法律法规的实施普及，此类现象一定会得到改善。

# 附录

## 数据来源

本次报告中涉及的所有数据，来源于 FreeBuf 数据、腾讯云大禹数据、云鼎实验室全球威胁情报监控平台数据，以及网络公开数据。大禹提供了攻击统计数据及真实 DDoS 案例，便于更为全面的呈现 DDoS 攻击流量及特性；云鼎实验室提供了 DDoS 新技术与溯源数据，便于呈现 DDoS 的最新发展技术与 botnet 的相关统计；同时 FreeBuf 从黑产链条角度直观地阐述了 DDoS 的黑产发展。这些数据结合腾讯和 FreeBuf 的深入分析与挖掘，让本报告得以从 DDoS 的新技术、新趋势、新黑产链等角度立体化呈现 DDoS 威胁与黑灰产业现状。

## 分析方法

本报告的流量数据分析基于业界公认的 NetFlow 协议进行，便于分析 DDoS 攻击及流量构成、分布及具体攻击行为。其中时间分布、地域分布等以监控到的中国及全球攻击总流量统计数据为基础，进行多维度多层次关联分析；而案例型分析与数据以典型攻击为例，基于单个事例的流量分析攻击手法和特征等。

# 参考资料

[1] 腾讯安全云鼎实验室：2018上半年互联网 DDoS 攻击趋势分析
http://www.freebuf.com/paper/174478.html

[2] Booters with Chinese Characteristics: The Rise of Chinese Online DDoS Platforms
https://blog.talosintelligence.com/2017/08/chinese-on-line-ddos-platforms. html

[3] The Growth of DDoS-as-a-Service: Stresser Services
https://blog.radware.com/security/2017/09/growth-of-ddos-as-a-service-stresser-services/

[4] DDoS-As-A-Service Popular on the Darknet
https://darkwebnews.com/dark-web/ddos-service-popular-darknet/

[5] DDoS 黑产调研
http://www.hackdig.com/11/hack-41179.htm

[6] 每秒470G！中国博彩公司遭遇罕见多矢量 DDoS 攻击
https://www.easyaq.com/news/523200148.shtml

[7] 动手搭建 DDoS 演练：揭秘在线 DDoS 攻击平台
http://www.freebuf.com/news/107916.html

[8] 在线 DDoS 搭建
http://blog.51cto.com/superwolf/1912767

[9] 英国一黑客16岁就开始在暗网兜售 DDoS 攻击工具
https://www.cnbeta.com/articles/tech/491141.htm38

[10] 38万人黑产帝国 DDoS 攻击利益链年入100亿
www.aqniu.com/industry/12052.html

# 关于报告

## 作者

**FreeBuf研究院:** 鲍弘捷、朱嘉豪、施东奇、余桂茗

**腾讯安全云鼎实验室：** 宋兵

**特别顾问：** 斗象科技能力中心（TCC）

**美术设计:** 王成

# 深渊背后的真相之「DDoS威胁与黑灰产业调查报告」


云鼎实验室
YUNDING LAB

FREEBUF
WWW.FREEBUF.COM