

DDoS

攻击商业破坏力

研 究 报 告



360


威胁情报中心

摘要

- 2015 全年，360 威胁情报中心共监测到全球网络 DDoS 攻击 27489410 次，被攻击网站数量多达 776095 个，平均每个被攻击的网站遭遇 DDoS 攻击 35.4 次。
- 从被攻击次数来看，约 33.7%（三分之一）的被攻击网站为没有 ICP/IP 备案的非法网站，这些非法网站提供的服务主要是游戏私服、色情信息和网上赌博等。排在第二位的被攻击网站类型是在线服务类网站，占比为 27.5%，主要包括门户网站、新闻网站和生活服务类网站等。
- 通过对被攻击网站持续一个月的流量检测，仅有不到一半（49%）的网站能够摆脱 DDoS 攻击的影响，恢复攻击之前的正常水平。而有约近四分之一（23%）的网站无法摆脱 DDoS 攻击的致命影响，基本无望重新复活。总体来看，DDoS 攻击过后，平均约每四家网站就会有一家被彻底打死。
- 分析显示，DDoS 攻击全年给网站经营者造成的经济损失至少为：投入成本损失 \approx 17.8 亿；商业价值损失 \approx 178.5 亿。流量收入损失不低于 1.67 亿元。
- 在所有 DDoS 攻击中，70.5% 的攻击带宽小于 1Mbps，而小于 10Mbps 的攻击占比接近 90%。100Mbps-1Gbps 的攻击仅占 2.2%，而大于 1Gbps 的攻击则仅占 0.2%。
- 从攻击时长来看，三分之二的 DDoS 攻击持续时间小于 10 分钟，而持续时间在 10 分钟至 1 小时的攻击占比约为 30.5%，持续时间超过 1 小时的攻击占比仅为 0.1%。
- 从精准性看，约有两成（17%）的 DDoS 攻击为高精度攻击，攻击时间与被攻击网站的业务流量高峰时段重合度在 80% 以上。另有 73% 的 DDoS 攻击时间与网站的业务流量重合度在 40%-70% 之间。总体而言，DDoS 攻击具有很强的策略性和针对性。
- 从僵尸网络攻击源看，在世界范围内（不含中国），南美洲的委内瑞拉和美国是最为主要的僵尸网络攻击源，在攻击源头中占比分别高达 33.4% 和 32.4%。其它的僵尸网络则主要集中在印度尼西亚、日本等亚洲国家。
- 从国内的僵尸网络情况来看，广东是僵尸网络最多的省级行政区，国内占比高达 14.5%。其次是浙江 7.7%，河南 6.3%，北京、四川紧随其后。

关键词

DDoS、经济

- 
- 2015 年全年，360 威胁情报中心共监测到僵尸网络主控服务器 13599 个。这些主控服务器是大量僵尸网络的控制者，可以称得上是僵尸网络中的僵尸王。
 - 有 45.0% 主控服务器会使用固定 IP 地址，而另外的 55.0% 的主控服务器则会使用固定域名。此外，约有 27.7% 的主控服务器的生存周期不满 1 天；生存周期在 2 天 – 一周的约占比 15.9%；生存周期在一周以上，一个月一下的为 22.1%。另有 7% 以上的主控服务器生存周期超过半年，更有 1.2% 的主控服务器生存周期超过一年。
 - 从端口来看，约有 16.7% 的僵尸网络主控服务器会选择一些特殊端口号来进行自我身份伪装。
 - 从主控服务器的全球地域分布来看，中美俄排名前三：44.3% 的主控服务器在中国境内；美国则是最大的海外控制源，占比为 19.8%；俄罗斯排第三，占比为 6.8%。
 - 从主控服务器的境内分布来看，江苏的主控服务器数量最多，占比为 27.6%；广东次之，占比为 17.5%，香港位列第三，占比为 8.3%。
 - 从技术角度看，SYN Flood 攻击仍然是最为主要的攻击方式，占 DDoS 攻击总量的 55.6%，超过半数；其次是 UDP Flood，占比为 37.5%，其中绝大多数为 AMP 攻击；DNS Flood 占比为 5.78%。
 - 从 24 小时分布看，SYN Flood 与 AMP (UDP Flood) 攻击在一天 24 小时中的分布都比较均匀，并没有攻击量特别突出的时段，但 DNS Flood 则比较明显的主要集中在深夜和凌晨。
 - 360 威胁情报中心对僵尸网络及 DDoS 服务的黑产链条进行了长期监测和追踪分析。根据目前已经掌握的情报线索来看，DDoS 攻击黑色产业链上，从业人员大致可以分为四类：木马作者、网络黑客、地下承包商以及网络黑帮。据估计，DDoS 黑产的年收入应当在 1.18 亿元 – 2.59 亿元之间。平均而言（折中收入），应在 2.3 亿元人民币左右。

损失、精准攻击、僵尸网络、C&C



CONTENTS

○ 攻击目标

被黑网站八十万，非法服务超三成 1

○ 商业损失

四个网站死一家，损失接近两百亿 2

一、DDOS 攻击的死亡率

二、DDOS 攻击商业损失

○ 攻击强度

短时小量最多发，两成打击高精度 4

○ 僵尸网络

南美广东常出没，主控尸王一万三 6

一、僵尸网络地域分布

二、僵尸网络的操控

○ 技术方法

SYN FLOOD 是主流，DNS FLOOD 在深夜 11

○ 黑产分析

三十块钱打死你，包月服务更便宜 13

攻击目标

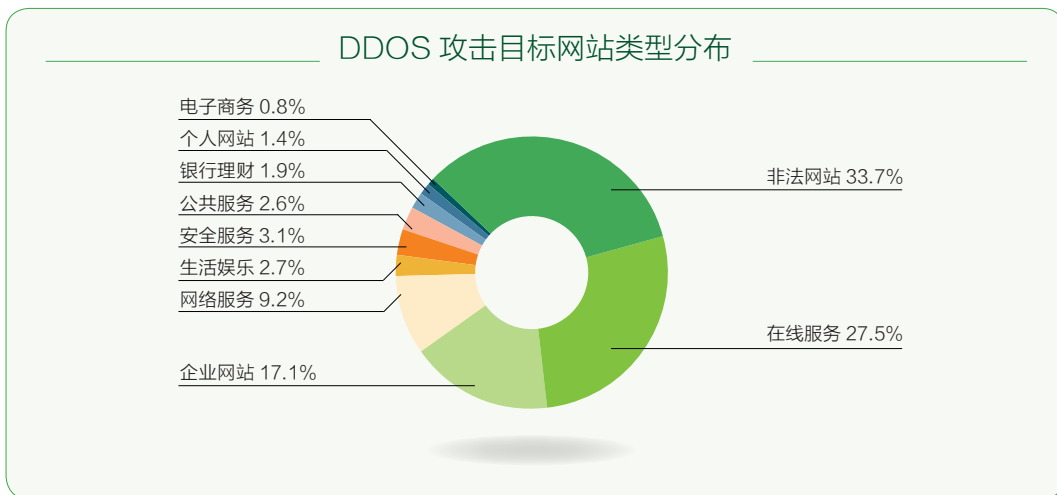
被黑网站八十万，非法服务超三成

2015 年，360 威胁情报中心共监测到全球网络 DDoS 攻击 27489410 次，被攻击网站数量多达 776095 个，平均每个被攻击的网站遭遇 DDoS 攻击 35.4 次。

通过对 2015 年 DDoS 攻击的抽样分析显示：从被攻击次数来看，约 33.7%（三分之一）的被攻击网站为没有 ICP/IP 备案的非法网站（不包括合法境外网站），数量占比最高。这些被攻击的非法网站提供的服务主要是游戏私服、色情信息和网上赌博等。排在第二位的被攻击网站类型是在线服务类网站，占比为 27.5%，主要包括门户网站、新闻网站和生活服务类网站等。排在第三至第五的网站类型分别是企业网站，网络服务和生活娱乐。详细信息参见表 1。其中，网络服务是指 DNS、CDN、云服务、大数据服务等基础网络服务。

所属行业	占比	说明
非法网站	33.7%	未备案的非法网站（主要为：游戏、色情、赌博等）
在线服务	27.5%	在线服务（门户、新闻、生活服务）
企业网站	17.1%	企业网站（企业主页）
网络服务	9.2%	网络服务（DNS、CDN、云服务、大数据服务）
生活娱乐	2.7%	生活娱乐（影视、音乐、游戏）
安全服务	3.1%	安全服务（网站防护、流量清洗）
公共服务	2.6%	公共服务（政府、教育、医疗）
银行理财	1.9%	银行理财（银行、理财、证券）
个人网站	1.4%	个人网站（个人主页、博客）
电子商务	0.8%	电子商务（电商、O2O）

表 1 DDoS 攻击网站类型分布



商业损失

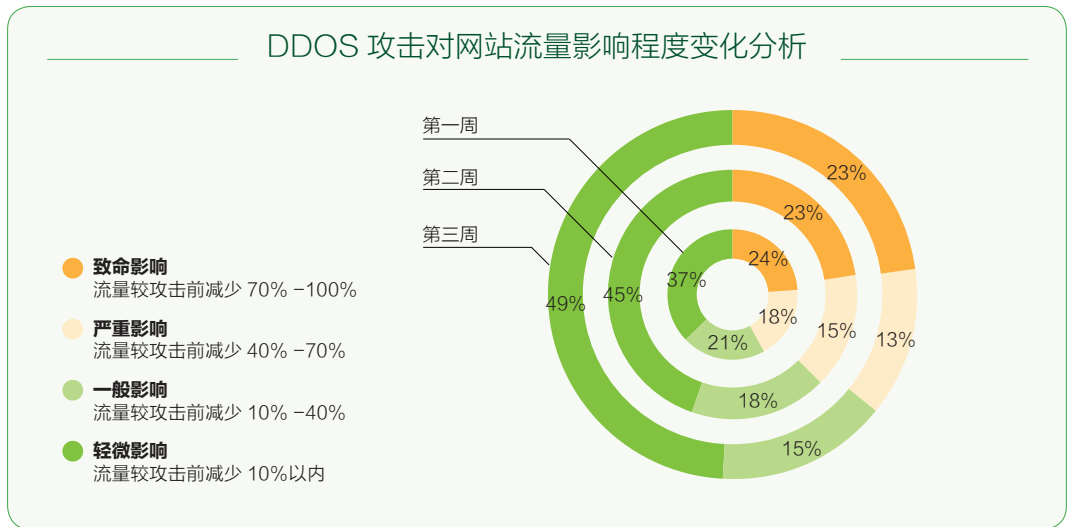
四个网站死一家，损失接近两百亿

一、DDoS 攻击的死亡率

360 威胁情报中心对部分遭遇 DDoS 攻击的网站进行了流量追踪抽样分析。统计显示，在遭遇 DDoS 攻击之后的一周时间里，约有 24% 的被攻击网站受到致命影响，日均流量较被攻击前的平均水平下降超过 70%；约 18% 的被攻击网站受到严重影响，流量下降在 40%–79% 之间；受 DDoS 攻击影响程度一般，流量下降在 10%–40% 的网站约占 21%；被攻击后仅受轻微影响，流量下降低于 10% 的网站约占 37%。

为进一步分析网站的自救与自我恢复能力，360 威胁情报中心又对部分被攻击网站的流量进行了为期 4 周（约 1 个月）的持续观测。结果显示，在其间没有遭遇新的 DDoS 攻击的情况下，尽管绝大多数被攻击网站的流量都呈现回升的态势，但也仅有不到一半（49%）的网站能够最终完全摆脱 DDoS 攻击的影响，网站流量能恢复到正常水平或受影响轻微。而且还有部分网站会出现流量加速下滑，病情不断恶化的情况，最终，仍有约近四分之一（23%）的网站无法摆脱 DDoS 攻击的致命影响，流量损失超过 70% 并且无法恢复，基本无望重新复活。总体来看，DDoS 攻击过后，平均约每四家网站就会有一家被彻底打死。

下图给出了 DDoS 攻击过后的 1–4 周时间内，被攻击网站流量损失的比例分布情况。





二、DDoS 攻击商业损失

鉴于 DDoS 攻击的主要原因是恶意竞争和敲诈勒索，所以被攻击的网站，即便只是中小网站，通常也是具有相当程度的商业价值。因此，结合前述统计，我们可以大致通过以下两个方面来评估 DDoS 攻击给整个互联网造成的经济损失。

1) 网站停服损失评估

若我们按照平均每个网站的搭建成本为 1 万元（包括网站设计、制作、设备、运维、推广等基本投入），商业价值为 10 万元（由广告收入、用户缴费收入等评估的网站资本价值）的较低水平来估算，2015 年遭到攻击的网站数量为 77.6 万个，约 23% 的网站被攻击后受到致命影响，面临停服风险，那么 DDoS 攻击全年给这些网站的经营者造成的经济损失至少为：

投入成本损失： $1 \text{ 万元} \times 77.6 \text{ 万} \times 23\% \approx 17.8 \text{ 亿}$

商业价值损失： $10 \text{ 万元} \times 77.6 \text{ 万} \times 23\% \approx 178.5 \text{ 亿}$

2) 流量收入损失评估

根据前述分析中网站遭遇 DDoS 攻击后受影响程度的分析推算，网站在遭遇 DDoS 攻击后第 1 周的平均流量下降程度应不低于 26.1%，第 4 周的平均下降程度也应不低于 22.8%。

第 1 周流量下降平均程度（下限）： $70\% \times 24\% + 40\% \times 18\% + 10\% \times 21\% = 26.1\%$

第 4 周流量平均下降程度（下限）： $70\% \times 23\% + 40\% \times 13\% + 10\% \times 15\% = 22.8\%$

若假设网站的日均收入与网站流量成正比，而被攻击网站在被攻击前的日均收入为 1000 元（较低估值），则在 2015 年，DDoS 攻击每天给所有被攻击的网站造成的流量收入损失至少应在 55.5 万元 - 45.8 万元之间。

第 1 周每天流量收入损失（下限）： $1000 \text{ 元/天} \times 26.1\% \times 77.6 \text{ 万} \div 365 \text{ 天} \approx 55.5 \text{ 万元}$

第 4 周每天流量收入损失（下限）： $1000 \text{ 元/天} \times 22.8\% \times 77.6 \text{ 万} \div 365 \text{ 天} \approx 45.8 \text{ 万元}$

据此推算，DDoS 攻击在 2015 年全年给网站经营者造成的流量收入损失不会低于：

流量收入损失（下限）： $45.8 \text{ 万元/天} \times 365 \text{ 天} = 1.67 \text{ 亿元}$ 。

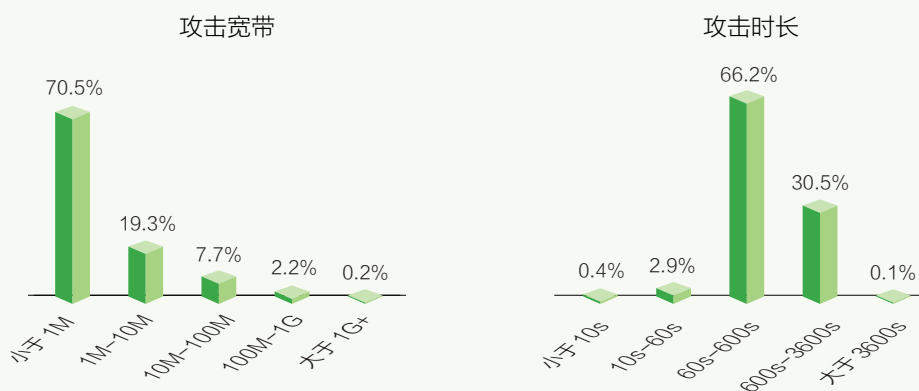
攻击强度

短时小量最多发，两成打击高精度

在 360 威胁情报中心监测到的所有 DDoS 攻击中，70.5% 的攻击带宽小于 1Mbps，而小于 10Mbps 的攻击占比接近 90%。100Mbps–1Gbps 的攻击仅占 2.2%，而大于 1Gbps 的攻击则仅占 0.2%。

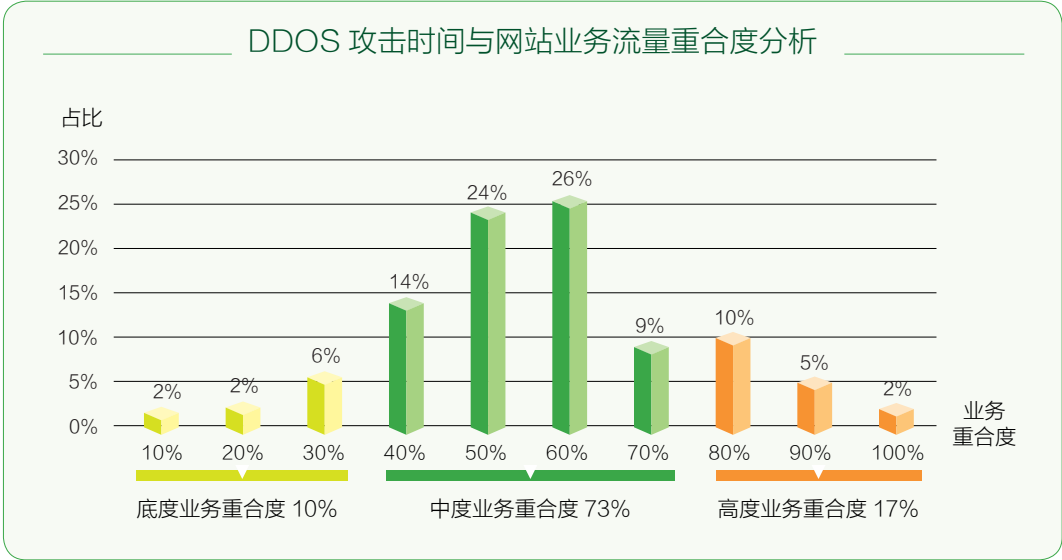
而从攻击时长来看，近七成的 DDoS 攻击持续时间小于 10 分钟，而持续时间在 10 分钟–1 小时的攻击占比约为 30.5%，持续时间超过 1 小时的攻击占比仅为 0.1%。总体而言，短时、小量的攻击仍然是 DDoS 攻击的主流。下图给出了 DDoS 攻击的带宽和时长分布统计。

DDoS 攻击的带宽与时长分布



为了进一步分析 DDoS 攻击的时间分布特性。我们对部分网站的业务流量峰值与 DDoS 攻击发生的时间进行了抽样比对分析。统计显示：约有两成（17%）的 DDoS 攻击为高精度攻击，攻击时间与被攻击网站的业务流量高峰时段高度重合，重合度在 80% 以上。另有 73% 的 DDoS 攻击时间

与网站的业务流量重合度在 40%–70% 之间。而业务重合度低于 30% 的 DDoS 攻击，仅占比 10% 左右。由此可见，DDoS 攻击具有很强的策略性和针对性。



僵尸网络

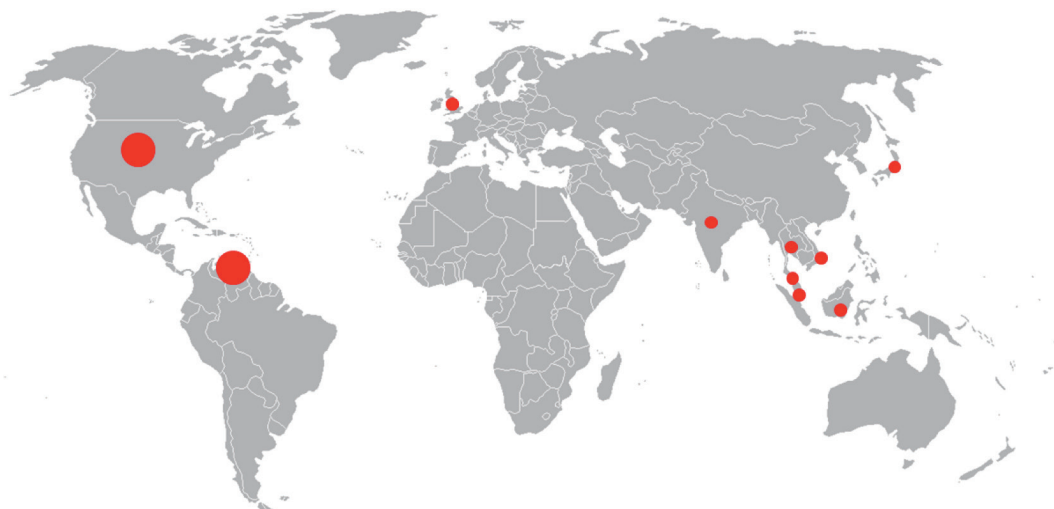
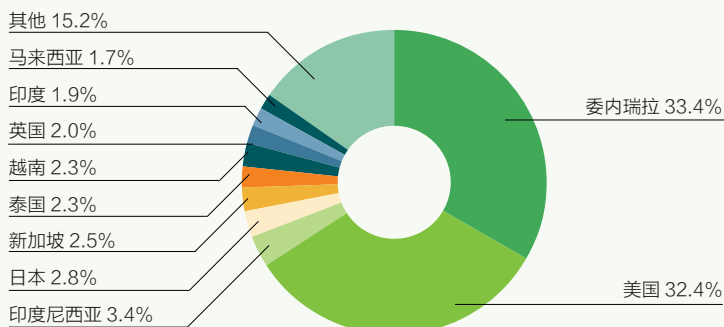
南美广东常出没，主控尸王一万三

一、僵尸网络地域分布

DDoS 攻击主要由受控的僵尸网络发动。统计显示，在世界范围内（不含中国），南美洲的委内瑞拉和美国是最为主要的僵尸网络攻击源，在攻击源头中占比分别高达 33.4% 和 32.4%。其它的僵尸网络则主要集中在印度尼西亚、日本、新加坡、泰国、越南、英国、印度、马来西亚。

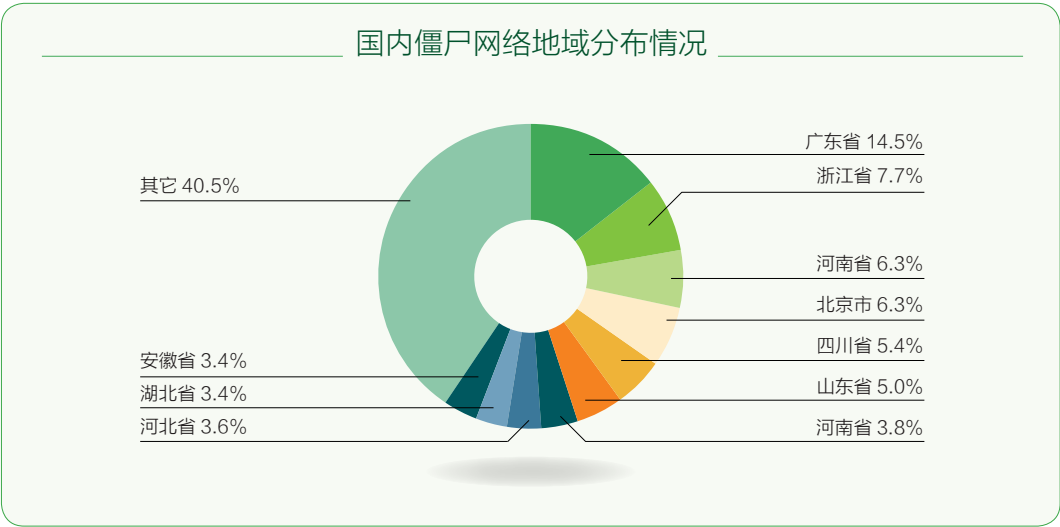
下面两图给出了全球僵尸网络的国家分布情况。

全球僵尸网络地域分布情况（不含中国）



而从国内的僵尸网络情况来看，广东是僵尸网络最多的省级行政区，国内占比高达 14.5%。其次是浙江 7.7%，河南 6.3%，北京、四川紧随其后。

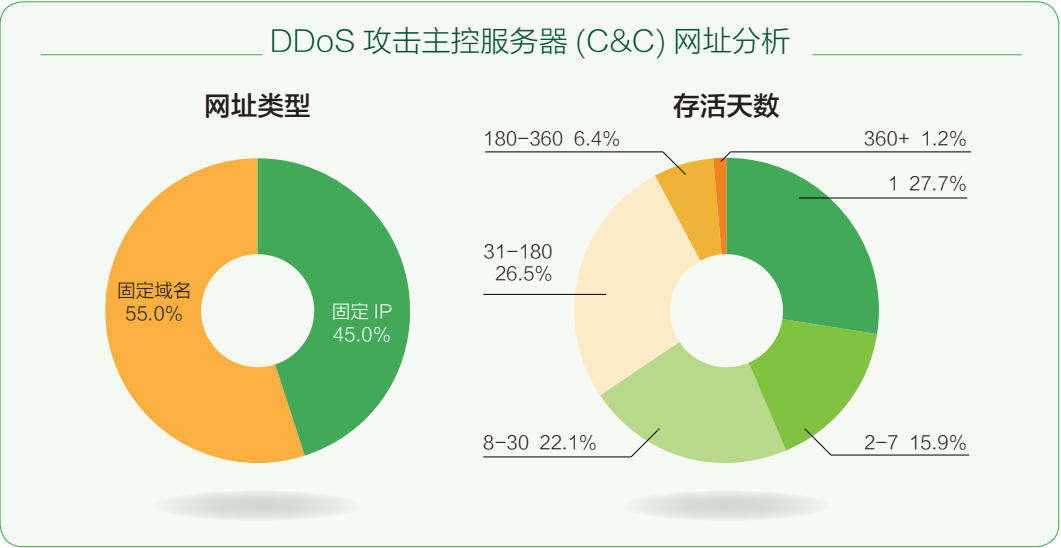
下面两图给出了国内僵尸网络的地域分布情况。



二、僵尸网络的操控

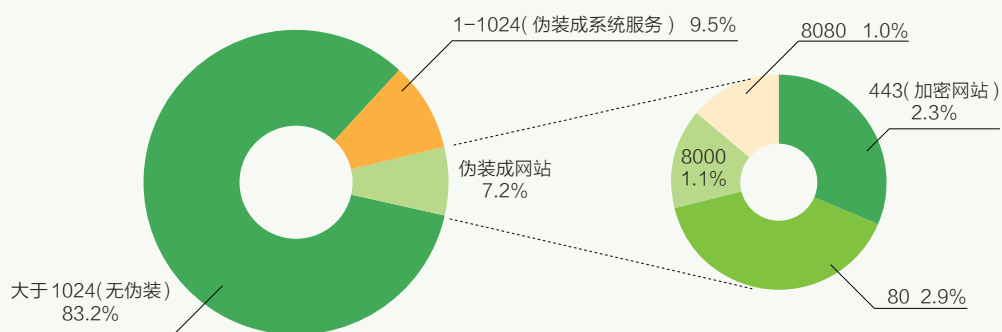
2015 年全年，360 威胁情报中心共监测到僵尸网络主控服务器 13599 个。这些主控服务器是大量僵尸网络的控制者，可以称得上是僵尸网络中的僵尸王。

通过对僵尸网络主控服务器的追踪分析显示：有 45.0% 主控服务器会使用固定 IP 地址，而另外的 55.0% 的主控服务器则会使用固定域名。此外，约有 27.7% 的主控服务器的生存周期不满 1 天；生存周期在 2 天至一周的约占比 15.9%；生存周期在一周以上，一个月一下的为 22.1%。另有 7% 以上的主控服务器生存周期超过半年，更有 1.2% 的主控服务器生存周期超过一年。总体而言，主控服务器的生存周期比一般的木马网站或钓鱼网站（生存周期通常不超过 48 小时）要长得多，这也就为我们定位、追踪僵尸网络提供了更多的机会。



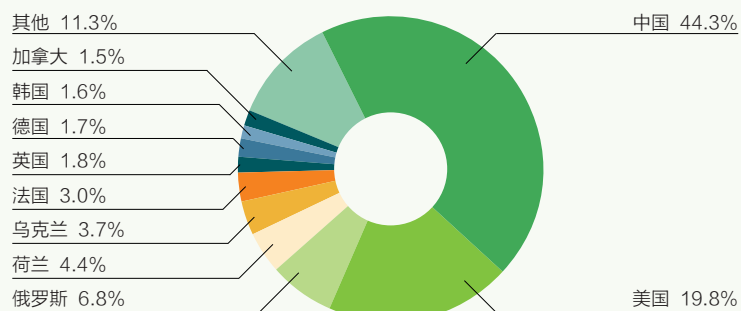
从端口来看，约有 16.7% 的僵尸网络主控服务器选择一些特殊端口号来进行自我身份伪装。其中，伪装成系统服务，即端口号在 1-1024 之间（不包括 80，443）的主控服务器占比为 9.5%，伪装成网站的（80、8000、8080、443 等）的为 7.2%：80 占 2.9%，8000 占 1.1%，8080 占 1.0%，443（伪装成加密网站）占 2.3%。

DDoS 攻击主控服务器 (C&C) 端口分析

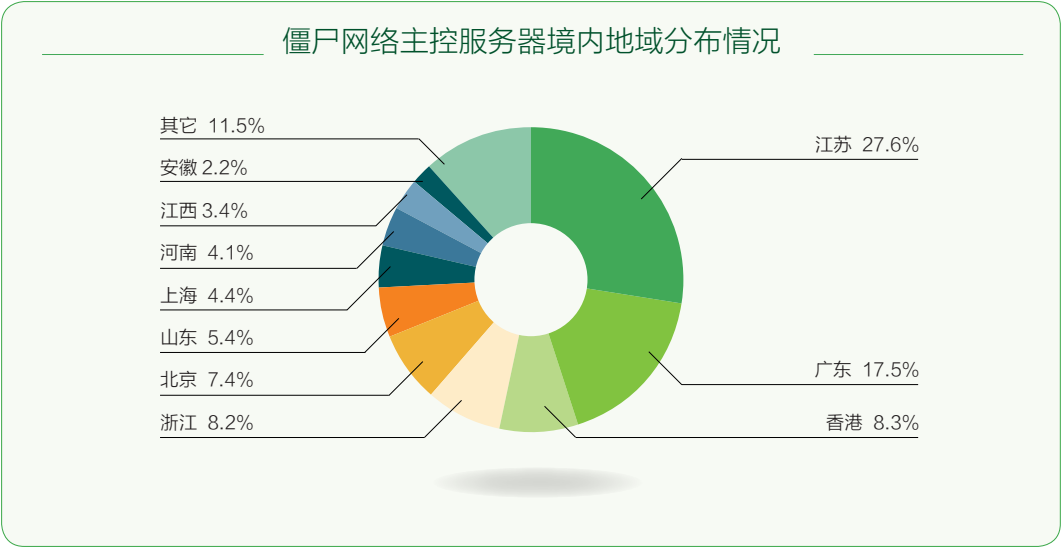


从僵尸网级主控服务器的全球地域分布来看,中美俄排名前三: 44.3% 的主控服务器在中国境内; 美国则是最大的海外控制源, 占比为 19.8%; 俄罗斯排第三, 占比为 6.8%。

僵尸网络主控服务器全球地域分布状况



从尸王级主控服务器的境内分布来看，江苏的主控服务器数量最多，占比为 27.6%；广东次之，占比为 17.5%，香港位列第三，占比为 8.3%。



此外，监测还显示，僵尸网络之间也存在着“黑帮械斗”和“联手结盟”的情况。我们即能看到几个分属不同派别的僵尸网络有相互攻击的明显迹象，同时也能看到分属不同派别的僵尸网络会在一定时间内突然同时对同一目标发动攻击。

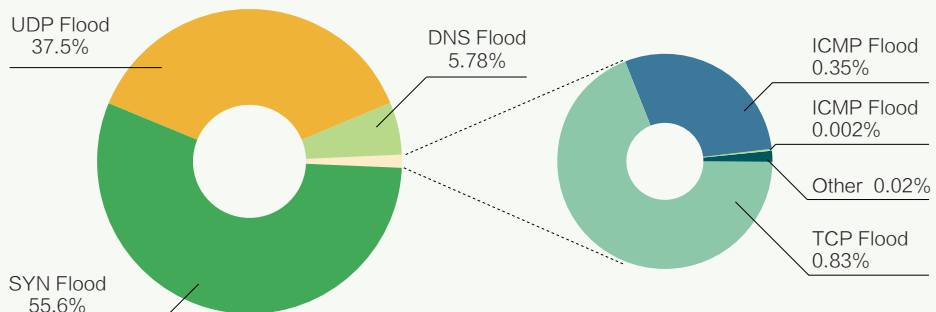
造成这种情况的主要原因有两个方面，一个是黑产之间本来就存着相互竞争与合作的关系；二是黑产的攻击行动往往取决于金主的需求和意图：同一个金主同时雇佣了不同派系的 DDoS 黑帮，不同派系的僵尸网络就会呈现出协同合作的态势；而相互斗争的金主分别雇佣不同派系的 DDoS 黑帮进行相互攻击，就有可能出现不同派系的僵尸网络相互攻击的情况。

技术方法

SYN Flood 是主流，DNS Flood 在深夜

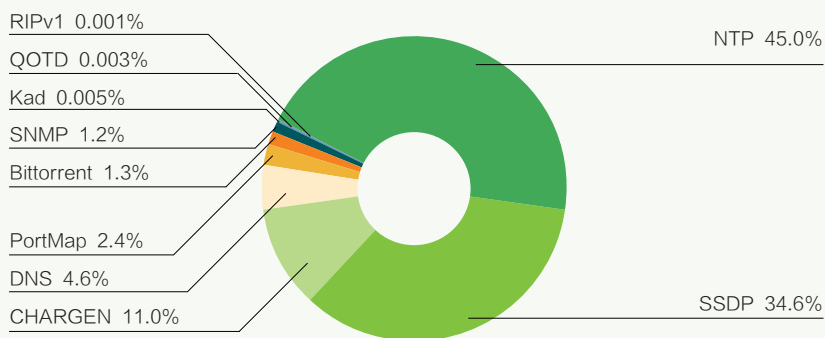
从技术角度看，SYN Flood、UDP Flood 和 DNS Flood 是最主要的三种攻击类型，从攻击次数来看，总占比接近 98.9%。SYN Flood 攻击仍然是最为主要的攻击方式，占 DDoS 攻击总量的 55.6%，超过半数；其次是 UDP Flood，占比为 37.5%，其中绝大多数为 AMP 攻击；DNS Flood 占比为 5.78%。

DDoS 攻击类型技术分析

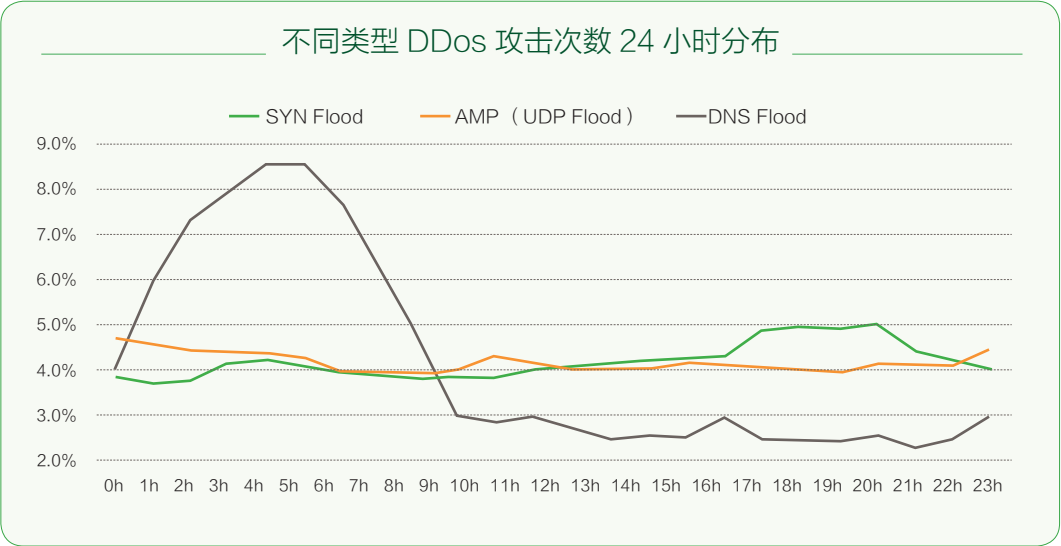


下图给出 AMP 攻击的一些细分类型的分布情况。其中，NTP 攻击占比最高，为 45.0%，其次是 SSD，占比为 34.6%，两者之和约占 AMP 攻击总量的 80%。

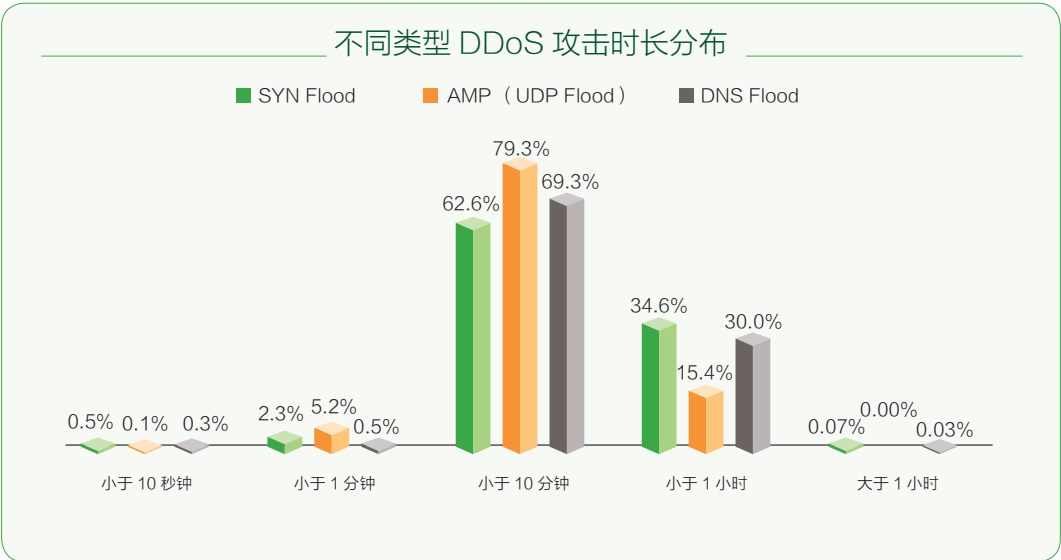
AMP 攻击细分类型分布



下图给出了不同类型 DDoS 攻击的 24 小时时间分布对比情况。其中可以看出，在 2015 年的 DDoS 攻击中，SYN Flood 与 AMP（UDP Flood）攻击在一天 24 小时中的分布都比较均匀，并没有攻击量特别突出的时段。但 DNS Flood 则比较明显的主要集中在深夜和凌晨。



下图给出了不同类型 DDoS 攻击的攻击时长分布对比。总体来看，不同类型的 DDoS 攻击，攻击时长的分布差异不大。

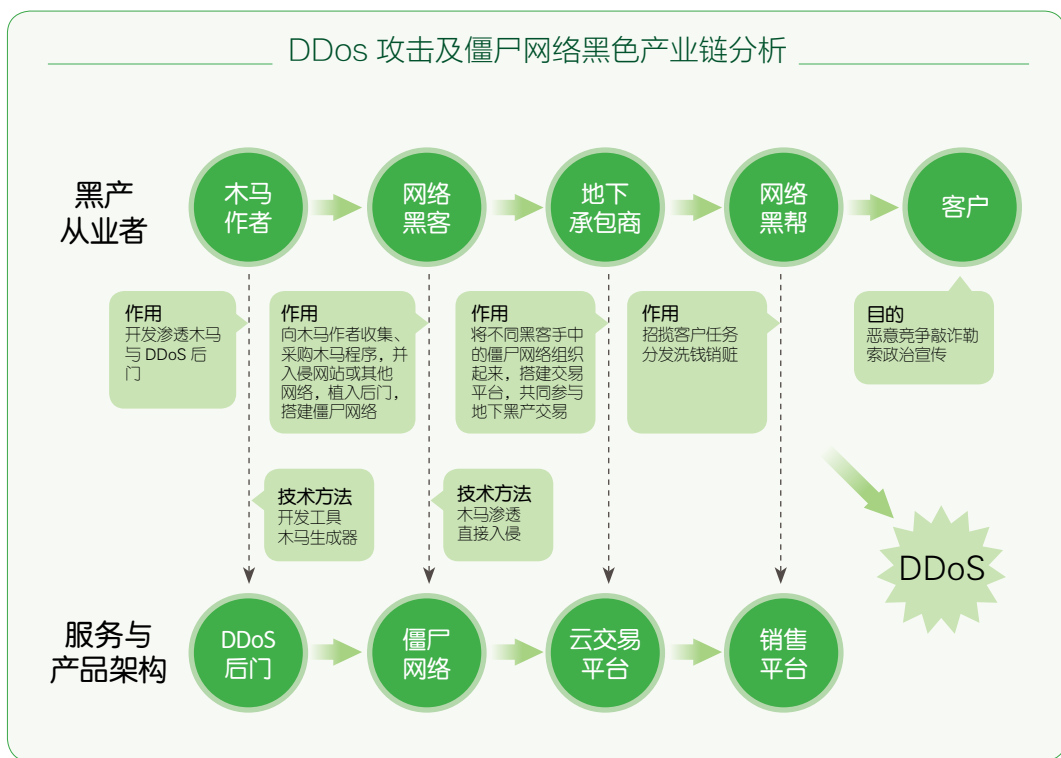


黑产分析

三十块钱打死你，包月服务更便宜

为了更进一步深入了解 DDoS 攻击的产业模式，360 威胁情报中心对僵尸网络及 DDoS 服务的黑产链条进行了长期监测和追踪分析。根据目前我们已经掌握的情报线索来看，DDoS 攻击黑色产业链上，从业人员大致可以分为四类：木马作者、网络黑客、地下承包商以及网络黑帮。而从 DDOS 攻击的产品和服务层次来看，黑色产业链又大致可以分为 DDoS 后门、僵尸网络、云交易平台和销售平台等几个不同的层次。

下图给出了 DDoS 攻击黑色产业链的基本模型分析。



木马作者：研发用于 DDoS 攻击的后门程序及网站渗透工具的人。这些人通常并不直接参与 DDoS 攻击，而是直接把自己研发的木马程序卖给专门从事各种网络攻击的其他黑客。

网络黑客：此处特指那些专门通过入侵网站或其他网络服务系统，并在其中植入 DDoS 攻击后门程序的黑客。这些黑客入侵网站的主要手段有两种：一是通过传播木马程序逐步渗透，并最终获取网站的控制权；二是利用网站漏洞，直接入侵网站并获取控制权。而一旦 DDoS 后门植入成功，相关网站或网络就成为了僵尸网络。

地下承包商：这是专门将网络黑客，以及黑客手中的僵尸网络组织起来参与 DDoS 攻击黑产活动的团伙。他们从下游的网络黑帮手中承接任务，并分派给上游指定的网络黑客，进而通过僵尸网络发动 DDoS 攻击。某些地下承包商还会搭建某种形式的交易平台，用于协调和组织网络黑客。

网络黑帮：专门在互联网上承揽各种 DDoS 攻击业务并收取服务费的黑帮团伙。网络黑帮收取服务费后还会进行洗钱及与上游各个环节进行分赃的工作。某些网络黑帮甚至会公然搭建销售平台或相关网页来承接各种用户业务。

下图就是我们在某个专门承揽 DDoS 攻击业务的网站上下载的一份收费清单。从图中可以看出，该平台提供的服务非常细致，可以根据攻击的带宽和攻击的天数来进行差异化的收费。最便宜的 50M 包日服务，仅需 30 元，100M 包月服务也只有 500 元。但这样的攻击，已经足以让某些中小网站被打瘫或打死。

同时，该平台还能提供 40G 以上的超大流量攻击，其包月服务价也只有 16800 元。而如果该平台确实能够提供 40G 带宽攻击的包月服务，那么可以说，绝大多数的中小网站，甚至是某些大型网站都一定会被打死。从这个意义上说，只要肯花 16800 元，你几乎可以“雇佣”杀死任何一家网站。

用户组	价 格	有效期	赠送积分	操 作
50M/日付	30元	1天	免费20分钟已升级日付:防止他人恶意浪费	立即开通
100M/月付	500元	30天	(100M/每秒) 全自动开通 无限流量 目标地址:IP	立即开通
1G/日付	100元	1天	(1G/每秒) 全自动开通 无限流量 目标地址:IP	立即开通
1G/月付	900元	30天	(1G/每秒) 全自动开通 无限流量 目标地址:IP	立即开通
5G/日付	300元	1天	(5G/每秒) 全自动开通 无限流量 目标地址:IP	立即开通
5G/月付	2800元	30天	(5G/每秒) 全自动开通 无限流量 目标地址:IP	立即开通
20G/日付	1150元	1天	(20G/每秒) 全自动开通 无限流量 目标地址:IP	立即开通
20G/月付	9800元	30天	(20G/每秒) 全自动开通 无限流量 目标地址:IP	立即开通
40G/日付	2000元	1天	(40G/每秒) 全自动开通 无限流量 目标地址:IP	立即开通
40G/月付	16800元	30天	(40G/每秒) 全自动开通 无限流量 目标地址:IP	立即开通
CC日付	300元	1天	(无视高防 无视CDN加速) 网站地址:http开头必填	立即开通
CC月付	2600元	30天	(无视高防 无视CDN加速) 网站地址:http开头必填	立即开通
高级版CC日付	600元	1天	(无视高防 无视CDN加速 增加五倍威力) 网站地址:http开头必填	立即开通
高级版CC月付	5500元	30天	(无视高防 无视CDN加速 增加五倍威力) 网站地址:http开头必填	立即开通

结合上面报价单以及 360 威胁情报中心在 2015 年对所有 DDoS 攻击的带宽、时长、频次分析，大致可以估算出 DDoS 攻击的网络黑产在 2015 年的基本收入或产业规模状态（不包括敲诈勒索的收入所得）。详见下表。

攻击流量 (M)	百分比	全年攻击次数	包日价(元)	包月 价 (元)	全包日服务 年收入估算	全包月服务 年收入估算	折中年收入 估算
小于 1M	70.50%	19379438	30	500	145345785	80747658	132426160
1M-10M	19.27%	5298543	30	500	39739073	22077263	36206711
10M-100M	7.74%	2127826	100	500	53195650	8865942	44329708
100M-1G	2.25%	617175	100	900	15429375	4628813	13269263
1G-5G	0.24%	63861	300	2800	4789575	1490090	4129678
大于 5G	0.00%	2567	300	9800	192525	209638	195948
总计	258691983	118019403	230557467				

表 2 DDoS 攻击产业年收入规模分析

下面简单说明一下全包日收入估算、全包月收入估算及折中收入估算的计算方法。

首先，统计显示，若以“日”为统计周期，那么在同一日内遭遇 DDoS 攻击的网站中，平均每个网站被攻击的次数约为 4 次。因此：

全包日服务年收入估算 \approx （全年攻击次数 \div 4） \times 包日价

全包月服务年收入估算 \approx （全年攻击次数 \div 4 \div 30） \times 包月价

再者，在实际市场中，肯定是有人购买包日服务，有人购买包月服务。但具体的比例分布，目前我们还不完全掌握。我们在上表中是使用了普遍适用的“二八原则”对黑产收入进行了估算，即，假设 80% 的金主会购买包日服务，而 20% 的金主会购买包月服务。因此：

折中年收入估算 \approx 全包日收入估算 \times 80% + 全包月收入估算 20%。

在上面表格中可以看出，如果所有的 DDoS 攻击都采用包日或包月的服务，那么，DDoS 服务的购买者在 2015 年向黑产支付的资金成本，也就是 DDoS 黑产的年收入应当在 1.18 亿元-2.59 亿元之间。平均而言（折中收入），DDoS 黑产年收入应在 2.3 亿元人民币左右。