DDoS 黑产调研

原创2016-11-18muzi

前不久发生的规模空前的网络攻击事件——诸多大型网站包括 Twitter、GitHub、PayPal、Tumblr、Pinterest、索尼 PS 网络、华尔街日报等等全都无法登陆，美国大半个互联网瘫痪，起因正是 DNS 服务提供商 Dyn 遭遇黑客大规模 DDoS 攻击，导致大量网站的 DNS 查询得不到响应，这也使得 DDoS 攻击再次成为热议的焦点。

基于此，本文对 DDoS 攻击黑客地下产业链展开了调查研究，从 DDoS 攻击目的，攻击的目标类型以及攻击造成的危害切入，进一步调查 DDoS 攻击地下产业链的交易渠道、攻击资源的获取以及黑产盈利方式等具体细节。

1. DDoS 简介：

1.1 DdoS 定义：

分布式拒绝服务攻击（Distributed Denial of Service）借助于客户/服务器技术，将多个计算机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（Denial of Service），从而成倍提高拒绝服务攻击的威力。

1.2 DDoS 攻击目的：

（1）商业恶性竞争：

商业竞争在互联网这个万亿市场中尤为激烈。一些行业竞争者为了利益不择手段、不顾法纪，通过 DDoS 攻击妨碍竞争对手的业务活动，打击对手的声誉，从中获取竞争优势。其中，电商行业和在线游戏行业是重灾区。

（2）敲诈勒索：

DDoS 由于成本低、实施容易等特点，在较早期就开始成为黑客在网络上进行敲诈勒索、收取“保护费”的主要方式。

1.3 DDoS 攻击目标以及造成的危害：

DDoS 攻击目标：非法网站占比三分之一

360 威胁情报中心 2015 年监测数据显示，全球网络遭受到 DDoS 攻击次数高达 27489410 次，其中约 33.7%（三分之一）的被攻击网站为没有在 ICP/IP 备案的非法网站，这些网站提供的服务主要是游戏私服、色情信息和网上赌博等等。其余详细信息参见下表：

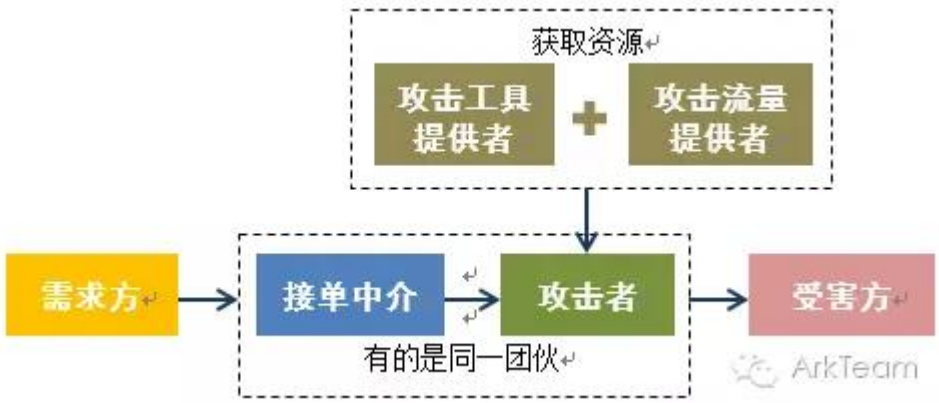
所属行业	占比	说明
非法网站	33.7%	未备案的非法网站（主要为：游戏、色情、赌博等）
在线服务	27.5%	在线服务（门户、新闻、生活服务）
企业网站	17.1%	企业网站（企业主页）
网络服务	9.2%	网络服务（DNS、CDN、云服务、大数据服务）
生活娱乐	2.7%	生活娱乐（影视、音乐、游戏）
安全服务	3.1%	安全服务（网站防护、流量清洗）
公共服务	2.6%	公共服务（政府、教育、医疗）
银行理财	1.9%	银行理财（银行、理财、证券）
个人网站	1.4%	个人网站（个人主页、博客）
电子商务	0.8%	电子商务（电商、O2O）

DDoS 攻击的死亡率：平均四个网站死一家

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%。这些被攻击网站在一个月内没有遭遇新的 DDoS 攻击的情况下，仅有一半（49%）的网站能够最终完全摆脱 DDoS 攻击的影响，流量能够恢复到正常水平或受轻微影响，但最终有近四分之一（23%）的网站无法摆脱 DDoS 攻击的致命影响，流量损失超过 70%，基本无望重新复活。总体来看 DDoS 攻击过后，平均每四家网站就会有一家被彻底打死。

2. DDoS 攻击地下产业链：

现如今 DDoS 的产业链条已经发展得十分成熟。各团伙之间分工明确、合作紧密，俨然形成一个井然有序、不断扩张的地下市场。下图展示了 DDoS 攻击地下产业链整体结构以及各部分的分工。需求方将攻击需求告知接单中介，由接单中介招募攻击者对指定的受害方发起 DDoS 攻击。其中还有很重要的一环就是攻击者需要从拥有工具或流量的第三方获取攻击资源，才能发动攻击。



黑产中往往通过一些行话术语作为关键字来构建广告信息，知晓黑产中行话是了解黑产的第一步，下面对 DDoS 黑产中行话进行简要解释： “D 单”是指 DDoS 攻击；“C 单”是指 CC 攻击（Challenge Collapsar，是指攻击者借助代理服务器生成指向受害主机的合法请求，利用身份伪装实现对受害主机的 DDoS 攻击）； “包天单”是指雇佣黑客在白天攻击网站；“包夜单”则是雇佣黑客在晚上实施攻击；“肉鸡”是指被攻击者取得完全控制权的主机；“抓鸡”是指通过端口扫描或者漏洞利用等方式取得主机的控制权。

2.1 交易渠道：

中国互联网中，DDoS 交易渠道主要包括 Web 论坛和 QQ 群两类。

(1) Web 论坛

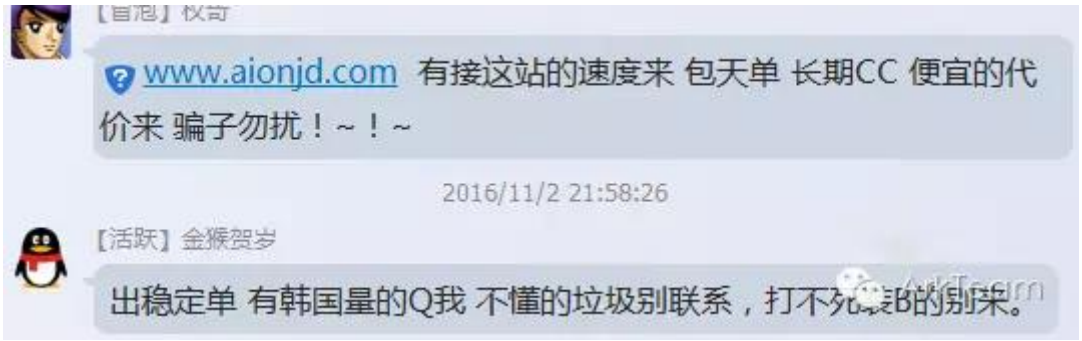
百度贴吧作为中国互联网最大的中文社区，提供了基于关键字的贴吧组织方式以及便捷的登录与发帖机制，吸引了大量黑产从业者，DDoS 吧就是其中的一类，如下图，黑产人员会在帖吧中发布 DDoS 广告信息，并附上 QQ 号码方便进一步交易协商。

(2) QQ 群

大部分 DDoS 交易还是基于 QQ 群方式，黑产 QQ 群一般通过在 Web 论坛中发布群号与业务类型，或是在 QQ 群名和描述中包含行话术语，我们可以通过在 QQ 中直接查找行话术语找到所需要的交易信息。

QQ 中搜索 DDoS 关键字，共检索到 152 个 DDoS 群组，部分结果截图如下：

这些 QQ 群的运作方式也非常简单直接，买家和卖家根据需求直接在 QQ 群中发布广告信息，交易细节再进一步私聊协商。截图如下：



2.2 攻击资源的获取：

攻击资源主要有僵尸网络和网页端 DDoS 平台，对应的交易方式也是不同的。

(1) 僵尸网络：

僵尸网络（Botnet，也叫机器人网络）是指黑客将大量僵尸机器（就是平常所说的“肉鸡”）感染僵尸程序（Bot）病毒，从而在黑客和被控主机之间建立一个一对多控制网络，从而对特定目标发起 DDoS 攻击，大部分 DDoS 攻击由受控僵尸网络发动。

僵尸网络所使用的“肉鸡”主要分为远控服务器、PC 设备以及物联网设备三类。

远控服务器“肉鸡”主要是 G 口发包（即接入互联网的带宽是 1G 以上）的 Windows 系统（多开放 3389 端口）或 linux 系统的服务器，价格几元到几十元不等，分为国内远控服务器和国外远控服务器，交易过程中卖方提供服务器 ip 和端口，卖方可以根据管理员账号和密码进行控制。远控服务器“肉鸡”特点是配置高，流量大，实施 DDoS 攻击效果显著。

PC 设备“肉鸡”：包括所有可连网的个人 PC 机，特点是流量较小，配置较低，价格相对便宜，每只 0.08 元到 1 元不等，交易量较大，每次能达到上百只。

物联网设备（IoT，Internet of Things）“肉鸡”：物联网设备“肉鸡”包括家庭网络、路由器、调制解调器、CCTV 系统和工业控制系统。本文开头提到的美国大面积网络瘫痪事件正是物联网设备僵尸网络驱动的 DDoS 攻击所造成的，但物联网设备一旦断电重启后僵尸程序（Bot）就会失效，需要重新感染，因此这类设备具有一定的即时性，所以在论坛和 QQ 群中并没有这类“肉鸡”的交易信息，但相关人士称从事黑产的黑客已将所抓到的物联网设备“肉鸡”进行出售，近期美国大规模网络瘫痪事件可能只是一个测试。


Hackers offered an IoT botnet for $7,500. The recent attack may be just a test

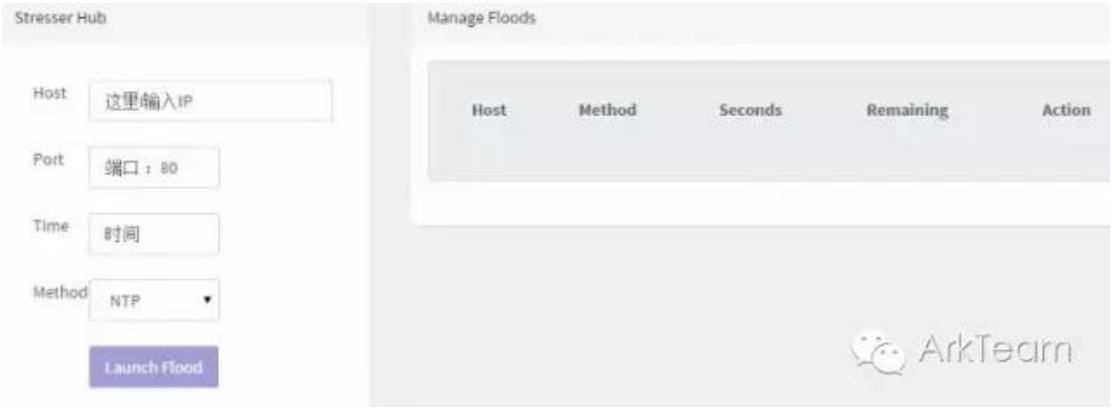
October 24, 2016 By Pierluigi Paganini

下表对“肉鸡”种类及交易细节进行汇总展示：

“肉鸡”种类	特点	价格（/只）		交易内容	交易方式
远控服务器	功能性强，流量大，价格较高	国内	2 元	机器 ip、端口，管理员账号密码	支付宝
		国外	15~60 元不等		
PC 机	流量有限，价格便宜，单次交易量较大	0.08~1 元不等			
IoT	断电重启 Bot 失效	--			

(2) 网页端 DDoS 平台：

网页端 DDoS 平台的后台是由大宽带高性能的集群服务器组成。由于通过抓“肉鸡”构建僵尸网络来获取流量耗时耗力，并且不够稳定，所以一些攻击者会选择流量大、性能相对稳定的网页版 DDoS 平台。网页端平台的使用非常便捷，只需登录平台，输入要攻击主机的 IP、端口和时间，选择攻击模式，即可发起攻击。网页端 DDoS 平台截图：



下面是网页端 DDoS 平台提供的交易信息，可以看出该平台提供各种不同等级的攻击套餐，不同的攻击套餐对应不同的价格，并且该平台可以使用 Bitcoin 支付，暂不支持 PayPal 支付。

上述常用 DDoS 网页端多为国外产品，可以通过国内中介代购国外网页端 DDoS 平台，代购信息同样通过 Web 论坛和 QQ 群发布。网页端 DDoS 平台国内代购攻击流量 3-5G 价格为数百元，流量 20G 以上价格往往可达到上千元，交易内容截图：

2.3 DDoS 黑产获利方式：

(1) 出售攻击工具和流量：

现在许多 DDoS 攻击的工具在网络上可以直接免费下载，但是一些功能较好的，有特殊定制服务的软件，还是需要从专业的制作团伙购买。软件作者一般会根据攻击团伙的需求，编写定制化软件，并收取费用。一般数百元到千元不等。流量买卖就是指上文提到的对“肉鸡”的买卖或者网页端 DDoS 平台的租用。

(2) 接单中介抽水：

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”、“包夜单”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。

(3) 攻击者攻击获利：

在这个黑色产业中，DDoS 攻击者不再是单纯发泄不满或炫耀技术的年轻人，也不再是组织攻击的主角，他们更多是“客户”所雇佣的“打手”。通过接单中介或自己直接接单，黑产从业人员的月收入可达到数万元人民币。

本文对 DDoS 攻击进行研究，从中可以看出现在的 DDoS 攻击是协奏、分布更为广泛的大规模攻击阵势，破坏能力也是空前的，这使我们更深刻地认识到仅仅依靠某种系统或硬防服务器来防御 DDoS 攻击是不够的，应当把防御 DDoS 做成一个系统工程，全面考虑并作出部署，才能起到有效的防御作用。

参考资料：

[1] http://www.freebuf.com/news/116629.html
[2] http://km623600.lofter.com/

[3] https://str3ssed.me/panel/register.php
[4]http://www.freebuf.com/articles/5104.html
[5]http://securityaffairs.co/wordpress/category/iot
[6] http://ti.360.com
[7]http://sec.chinabyte.com/185/13356685.shtml
[8] http://www.vsharing.com/k/net/2016-10/718660.html
[9] 《2015 H1 绿盟科技 DDoS 威胁报告》
[10] 《中国互联网信息安全地下产业链调查》

更多精彩内容，请关注：

1. ArkTeam 官方微信—公众账号名称：ArkTeam

2. ArkTeam 官方微博：

昵称：ArkTeam

网址：http://www.weibo.com/arkteam

http://mp.weixin.qq.com/s?__biz=MzA3Mjk4MDMzMQ==&mid=2648248330&idx=1&sn=feba8faceab95810f4c5e252487d6633