

# DDoS 攻击及主动防御模型研究

刘旭勇

(西北大学, 陕西 西安 710069)

**摘要:**DDoS(分布式拒绝服务)攻击正在对整个互联网产生巨大的危害和严重的经济损失,且不断增大。通过介绍 DDoS 攻击原理和分析 DDoS 攻击网络的控制机制,提出基于蜜网的防御 DDoS 攻击方法,鉴于目前大多数 DDoS 攻击都是黑客利用其控制的僵尸网络发起的,部署了改进版的蜜网,利用蜜罐收集的信息,打入黑客控制的僵尸网络内部,获取重要信息,切断黑客的远程控制机制,从根源上阻止 DDoS 攻击远程控制网络的形成,以达到主动防御的目的。

**关键词:**分布式拒绝服务;蜜网;僵尸网络;远程控制网络

**中图分类号:**TP393.08

**文献标识码:**A

**文章编号:**1673-629X(2008)07-0143-03

## Research on DDoS Attacks and Proactive Defense Model

LIU Xu-yong

(Northwest University, Xi'an 710069, China)

**Abstract:**DDoS (distributed denial of service) attack is doing great harm and serious economic loss for entire Internet, which become worse and worse. Puts forward the defense DDoS attack method based on honeynet after the concept of DDoS attack is introduced and the controlling mechanism of its attack network is analyzed. In view of the fact that most of DDoS attacks are from hackers who make use of the botnet of its control, announce the information that improves the honeynet and collects using honeypot. Therefore, it is important to enter the botnet inside of hacker control, get important information, cut off the remote control mechanism of hacker, and prevent building remote control network for DDoS attack from root-cause so that proactive defense is achieved.

**Key words:**distributed denial-of-service;honeynet;botnet;remote control network

## 0 引言

分布式拒绝服务攻击是拒绝服务攻击的一种演变。传统的拒绝服务攻击利用合理的服务请求来占用过多的服务资源,从而使合法用户无法得到服务响应。这种攻击方式随着计算机处理能力的逐步提高以及网络带宽的扩展,对系统的影响能力逐渐减少,在此基础上出现了一种新型的攻击方式,攻击者控制多台机器同时向一个目标主机或网络发起攻击,导致目标主机不能提供正常的服务或网络瘫痪,这就是分布式拒绝服务攻击。分布式拒绝服务攻击使防御的难度加大源于被攻击者在一定时间内收到的大量数据包不只是从一台主机发送来的,同时,由于攻击来自于范围广泛的IP地址,而且来自每台主机的少量数据包有可能被入侵检测系统忽略,所以使检测和防范变得愈加困难。

DDoS攻击主要针对较大的站点,自1999年来,许多著名网站如Yahoo、eBay、CNN等都曾遭受过这种攻击<sup>[1]</sup>,造成难以挽回的经济损失。

## 1 DDoS 攻击原理及常用对策

### 1.1 DDoS 的攻击原理

DDoS攻击主要采用如图1所示的三层客户机服务器结构。可以看到,攻击者控制多台主控端主机,主控端主机控制那些分布在网络中的代理端机器,通过这些代理端机器同时向被攻击主机发送大量的无用数据包,占用被攻击主机的系统资源和网络带宽,导致被攻击主机的资源耗尽或网络阻塞,使其瘫痪不能正常工作。

分布式拒绝服务攻击分为以下几个层次:

(1)攻击者所用的计算机是攻击主控制台,可以是网络上的任何一台主机,甚至可以是一个活动的便携机。攻击者可通过向主控端发送攻击命令,操纵整个攻击过程。

(2)主控端主机是攻击者非法侵入并控制的一些

收稿日期:2008-02-19

基金项目:国家自然科学基金重点资助项目(60433010)

作者简介:刘旭勇(1975-),男,陕西西安人,硕士研究生,工程师,研究方向为网络安全、软件工程等;导师:鱼滨,副教授,研究方向为软件工程、基于Internet的软件技术。

主机,这些主机还分别控制大量的代理主机。主控端主机被攻击者安装了特定的程序,因此它们可以接收攻击者发来的特殊指令,并且可以把这些命令发送到代理主机上。

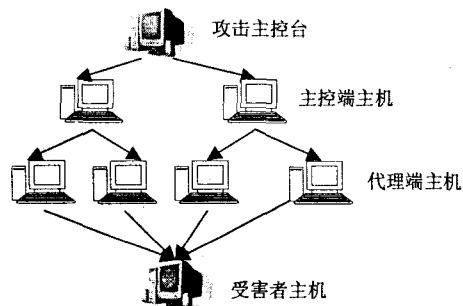


图 1 DDoS 攻击原理

(3) 代理端主机同样也是攻击者侵入并控制的一批主机,它们运行攻击程序,接收和运行主控端发来的命令。代理端主机是攻击的执行者,实施向受害者主机发送攻击。

攻击者发起 DDoS 攻击的第一步就是寻找在 Internet 上有漏洞的主机,进入该主机系统后在其上面安装后门程序,攻击者入侵的主机越多,他的攻击队伍就越壮大。第二步在入侵主机上安装攻击程序,其中一部分主机充当攻击的主控端,一部分主机充当攻击的代理端。最后各部分主机各司其职,在攻击者的调遣下对攻击对象发起攻击。由于攻击者在幕后操纵,所以在攻击时不会受到监控系统的跟踪,身份不容易被发现。

## 1.2 目前防御 DDoS 攻击的方法

近年来研究人员也提出多种防范措施,主要归结为两类:第一类方法是采取包过滤<sup>[2]</sup>、不允许广播包和关闭不用的服务或为系统打上安全补丁包<sup>[3]</sup>等措施,来减小影响;第二类方法是攻击源的识别和追踪<sup>[4]</sup>。过去几年中很多人研究如何确定出攻击者的攻击源:S. Savage 等使用包标记方案来使受害者反跟踪,查出发起包的确切位置<sup>[5]</sup>。D. Song 和 A. Perrig 通过使用网络拓扑图并减少标记数目的方法来提高追踪的效果<sup>[6]</sup>。上述方法在实施中或者需要网络拓扑信息(获得整个网络的拓扑信息是非常困难的),要求相关的 ISP 相互合作来完成追踪任务,中间要涉及众多分布于世界各地的网络机构,实施有一定的难度。

## 2 基于蜜罐的 DDoS 攻击主动防御方案

通过 DDoS 攻击的原理观察到 DDoS 攻击是许多主机并发的自动的攻击行为,而这些大量主机通常需要一种机制远程控制它们。为了阻止攻击,如果能识别、渗透、分析这种远程控制机制,然后以一种自动的、

控制的方式停止它,那么就有可能防御 DDoS 攻击。因此防御 DDoS 攻击的方法是影响,甚至切断远程控制机制,实施步骤如下:

- (1) 渗透远程控制网络;
- (2) 详细分析远程控制网络;
- (3) 切断远程控制网络。

在第一步,要在远程控制网络布置一个代理。这里的代理是指模拟成要渗透的远程网络的一个有效成员,代理必须用户化。例如,为了渗透僵尸网络,需要模拟一个僵尸工具甚至模拟一些僵尸命令。一旦能成功安装一个代理到远程控制网络,就可以进行第二步了,详细观察网络。可以开始监控所有的活动,分析所收集的信息。在最后一步,利用收集的信息切断远程控制网络。一旦成功切断远程控制网络,就能有效避免 DDoS 攻击的危险。

但此方法的难点是如何自动渗透网络以及分析过程,在一些案例中,代理端主机需要在代理端主机之间和攻击者之间建立起一种通信频道,如果能以一种受控制的方法“抓获”恶意软件,就有可能以自动的方式从恶意软件里提取出大量的有用的信息。以下介绍的基于蜜罐技术的方案能有效跟踪和收集网络的相关信息。

蜜罐(honeypot)技术是一种新兴的网络安全技术,它的实质是网络欺骗或网络陷阱,主要用于研究黑客攻击行为包括攻击策略、工具和动机,进而达到防御攻击的目的<sup>[7]</sup>。蜜罐系统是一个包含漏洞的用于网络诱骗的计算机系统,它通过模拟一个或多个易受攻击的主机,给攻击者提供一个容易攻击的目标。物理上通常是一台运行单个操作系统或借助于虚拟化软件运行多个虚拟软件的“牢笼”主机。装有多个系统和应用软件且高度相互作用的蜜罐所构成的网络,即为蜜网(honeynet)。其主要目的是收集黑客的攻击信息。但与传统蜜罐技术的差异在于,蜜网构成了一个黑客诱捕网络体系架构,在这个架构中,可以包含一个或多个蜜罐,同时保证了网络的高度可控性,以及提供多种工具以方便对攻击信息的采集和分析。

蜜网具有三大核心需求:数据控制、数据捕获和数据分析<sup>[8]</sup>。通过数据控制能够确保黑客不能利用蜜网危害第三方网络的安全,以减轻蜜网架设的风险;数据捕获技术能够检测并审计黑客攻击的所有行为数据;而数据分析技术则帮助安全研究人员从捕获的数据中分析出黑客的具体活动。

图 2 是提出利用蜜网实现 DDoS 主动防御的网络拓扑结构图。

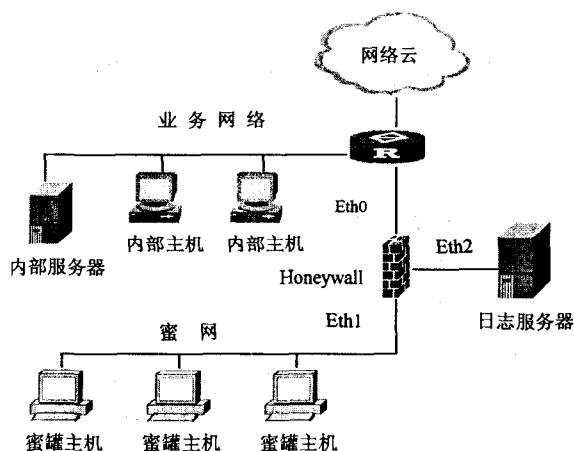


图2 DDoS主动防御拓扑图

这是一个改进版的蜜网体系,其中的Honeywall为一个没打补丁的Windows2000或者WindowsXP。因为这个系统非常容易导致被攻击,所以比较容易受到黑客的青睐,也使得比较容易收集防御DDoS攻击所需的信息,在整个部署中最为重要的是以桥接模式部署的蜜网网关(Honeywall),Honeywall包括三个网络接口,其中eth0连接外网,eth1连接蜜网,两个接口以桥接方式连接,不会对网络数据包进行TTL递减和网络路由,也不会提供本身的MAC地址,因此对攻击者而言,Honeywall是完全不可见的,同时Honeywall是蜜网与其他网络连接的唯一连接点,所有流入流出蜜网的网络流量都将通过Honeywall并受其控制和审计。Honeywall的另一网络接口eth2连接日志/控制服务器,使得捕获的数据能够发往日志服务器,同时也使得能够远程对Honeywall进行控制,该接口一般使用内部IP,并严密防护。

本蜜网DDoS防御机制及策略如下:

1)Honeywall捕获数据并将其发往日志服务器。包括:(1)防火墙的日志记录IPTab,IPTab防火墙记录的内容主要包括:数据包通过时间、包协议类型、进出的网络接口、源地址、目的地址、源端口、目的端口、包长度;(2)Eth1上的嗅探器记录的网络流,以PCAP格式存储,部署中用snort实现嗅探器功能,PCAP文件格式如表1所示。

表1 PCAP文件格式

文件头							数据包头			数据报
标识位	主版本号	副版本号	区域时间	精确时间戳	数据包最大长度	链路层类型	时间戳	数据包长度	数据包实际长度	

2)使用IPTab防火墙提供外出流量限制和使用网络入侵防御系统对已知攻击进行无效化。外出流量限制机制通过IPTab限制每台蜜罐主机在单位时间内允许向外发起的连接数以及流量速率,一旦攻击者利用

攻陷的蜜罐向外发起扫描、拒绝服务攻击等,Honeywall上的IPTab将丢弃超过限制的外出数据包,并产生警告通知,从而不会对第三方网络构成危害。

3)网络入侵防御系统则通过著名开源网络入侵检测系统snort工具实现,通过查看外出的每个数据包,发现其中包含的已知攻击特征,将生成警报并根据配置选择丢弃数据包或修改数据包使得攻击无效。

4)IPTab将记录所有的流入蜜网的网络连接,并记录攻击者攻陷蜜网后向外发起的网络连接以及超过连接数和流量速度限制的报警。

5)在Honeywall上部署的网络入侵检测系统snort将在eth1接口上监听全部流入流出蜜网的网络流量并抓取到本地的pcap文件中,并且对其中符合snort攻击特征的数据包产生报警日志,这些数据为追查并还原一个攻击行为提供了全面的网络流量信息。

6)攻击者通常会在攻击过程中使用SSH等加密信道发出攻击指令,而Honeywall提供的数据捕获机制即使将全部的数据包都截获并监听下来,也不能够了解其中所包含的攻击行为。但这些加密流量最终会在蜜罐主机上接收并进行解密,所以可以在蜜罐主机上安装一个系统行为监视器来对攻击者通过加密信道进行的攻击行为进行捕获。

以上方案在陕西行政学院计算机中心实施,取得了较好的主动防御效果。

### 3 结束语

文中介绍了一种防御DDoS攻击的方法,它在分析攻击者建立远程控制网络机制的基础上,利用蜜网技术诱骗、跟踪攻击者,在获取远程控制网络的主要信息后,使远程控制机制失效。它不依赖于资源优势也不需要增加额外的设备,从DDoS攻击体系的躯干入手而不是只着眼于攻击体系末端的防御,因而能更加有效地从整体上抵御DDoS攻击,是一种很有前景的主动防御方案。

#### 参考文献:

- [1] Harrison A. The Denial-of-service Attack Aftermath[EB/OL]. 2000. <http://www.cnn.com/2000/TECH/computing/02/14/dos.attempt.idg>.
- [2] Cisco Systems Inc. Defining Strategies to Protect Against TCP SYN Denial of Service Attacks[EB/OL]. 1999-07. <http://www.cisco.com/warp/public/707/4.html>.
- [3] Ferguson P, Senie D. Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing[S]. RFC2267, 1998.

(下转第152页)

要考虑每次读写合理的数据量,这样的处理会较好。

### 2.3 对数据库数据的整理和分类

随着时间不断推延,数据库应用系统中某些表的数据也在很快地累积,有时数据量还是比较庞大的。比如一个中等城市供电公司每月用户的抄表数据就有几万条甚至几十万条,虽然采用分布式数据库系统,通过分散处理再集中汇总的方式来解决数据量暴增的问题,但将大大增加各种费用和管理工作量<sup>[5]</sup>;如采取集中管理方式而又没有相应的措施,那将会使系统的负担越来越大,效率越来越低,最终会拖垮整个系统。

针对这种情况,需要在数据库设计时就要预见到,否则将会给后续的开发环节带来很大的麻烦。具体解决时,还要对具体的实际情况进行分析。就上面问题,在集中管理方式下可采用如下的解决方案:由于抄收表的数据量会很大,增长也很快,根据实际情况把相应的数据分类后建相应的表用于存放数据。例如在对每户电表抄表后,用户需要交费,可以把这些数据分为两类:欠费数据信息——存放在欠费表中;交费数据信息——存放在交费历史信息表中,这样可以使交费处理的时候查询量大大减小。由于交费历史信息表中的数据信息还是很庞大的,更进一步采取的措施是按月、季或年为时间单位建立新表,把交费历史信息表中相应的月、季或年的数据放到相应的表中,并编制具有灵活的条件组合查询或模糊条件查询功能的客户端程

序,这样就可以大大提高数据的查询效率。基于这样的考虑,可以在客户端加入数据整理和分类的功能菜单。

### 3 结束语

数据库应用系统的开发首要的任务是对于需求的充分分析,在此基础上预见性地考虑并解决系统高效率的瓶颈问题就成为关键。文中介绍的一些提高系统性能的方法和技术不但适用于中小的系统,更是适用于大型的数据库应用系统。这些方法的综合应用可以解决各种复杂系统的性能问题,能大大地提高数据库存取、查询等效率。

#### 参考文献:

- [1] 萨师煊,王 珊.数据库系统概论[M].北京:高等教育出版社,2003.
- [2] 陶 勇,丁维明.数据库中规范化与反规范化设计的比较与分析[J].计算机技术与发展,2006,16(4):107-109.
- [3] 邓 曦,卢正鼎,张 巍,等.多数据库系统查询优化算法的研究[J].小型微型计算机系统,2004,25(3):451-454.
- [4] 孔 哲,孟丽容.数据库连接策略优化方法[J].山东大学学报:工学版,2003,33(6):652-657.
- [5] 贾 焰,王治英,韩伟红,等.分布式数据库技术[M].北京:国防工业出版社,2003.

(上接第 145 页)

- [4] 蔡 杰,熊齐邦.DDoS 攻击下的 IP 追踪技术[J].计算机技术与发展,2007,17(3):159-162.
- [5] Savage S, Wetherall D, Karlin A, et al. Practical Network Support for IP Traceback[C]//In Proceedings of ACM SIGCOMM. [s.l.]:[s.n.],2000.
- [6] Song D, Perrig A. Advanced and Authenticated Marking

Schemes for IP Traceback[C]//In Proceedings of ACM INFOCOM. [s.l.]:[s.n.],2001.

- [7] Oudot L. Fighting Internet Worms with honeypots[EB/OL]. 2003. <http://www.securityfocus.com/infocus/1740>.
- [8] 诸葛建伟.蜜罐及蜜网技术简介[EB/OL]. 2004. <http://www.honeynet.org.cn/reports/蜜罐及蜜网技术简介>.

(上接第 148 页)

设都提供了很好的参考,具有较高的实用性和一定的社会价值。

#### 参考文献:

- [1] 宋金玲,肖 寒,盛业华. GIS 在数字校园建设中的应用[J].北京测绘,2002,4(3):10-12.
- [2] 孟令奎,史文中,张鹏林.网络地理信息系统原理与技术[M].北京:科学出版社,2005.
- [3] 杨祖虎. Arc IMS 初级教程[M]. 北京:ArcInfo 中国技术咨

询与培训中心,2001.

- [4] 黄丙湖,闫国年,张亦含,等.基于 ArcIMS 的环保 WebGIS 的设计与实现[J].南京师范大学学报:工程技术版,2004,4(2):59-61.
- [5] 杨晨毅,刘吉平.基于 SDE 的 GIS 空间和属性数据在 RDBMS 中的集成[J].计算机仿真,2003,20(11):110-112.
- [6] 窦长娥,刘仁义,刘 南.基于 ArcIMS 的旅游地理信息系统设计与实现[J].计算机应用研究,2006(2):160-165.