DDOS
分布式拒绝服务攻击

By Haisu

分布式拒绝服务攻击的实施及预防措施

攻击

- 1) 分布式拒绝服务攻击(DDoS)的概念以及它与拒绝服务攻击的区别。
- 2) DDoS攻击的过程和攻击网络结构。
- 3) DDoS攻击所利用的协议漏洞
- 4) DDoS的几种攻击方式
- 5) 一种新的DDoS攻击方式——反弹攻击

防御

- 1) DDoS攻击的防范原理。
- 2) DDoS攻击发生时网络出现的异常情况。
- 3) 防范中的软硬件使用
- 4) 拒绝服务监控系统的设计

DDoS的诞生

- 1999年8月以来，出现了一种新的网络攻击方法，这就是分布式拒绝攻击（DDoS）。之后这种攻击方法开始大行其道，成为黑客攻击的主流手段。Yahoo、eBay、CNN等众多知站点相继被身份不明的黑客在短短几天内连续破坏，系统瘫痪达几个小时甚至几十个小时之久。

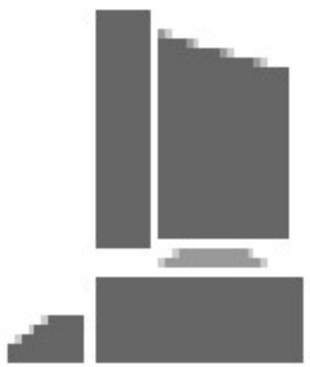
拒绝服务攻击

- 拒绝服务攻击（Denial of Service）——是一种个人或多人利用Internet协议的某些漏洞，拒绝其他用户对系统和信息的合法访问的攻击。
- 这类攻击使服务器充斥大量要求恢复的非法用户的信息和请求，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至瘫痪而停止提供正常的网络服务。

被DDoS攻击时的现象

- 被攻击主机上有大量等待的TCP连接
- 网络中充斥着大量的无用的数据包，源地址为假
- 制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯
- 利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求
- 严重时会造成系统死机

正常访问



通过普通的网络连线，使用者传送信息要求服务器予以确定。服务器于是回复用户。用户被确定后，就可登入服务器。

TCP三次握手方式

“拒绝服务”（DoS）的攻击方式

“拒绝服务”的攻击方式为：用户传送众多要求确认的信息到服务器，使服务器里充斥着这种无用的信息。 所有的信息都有需回复的虚假地址，以至于当服务器试图回传时，却无法找到用户。服务器于是暂时等候，有时超过一分钟，然后再切断连接。服务器切断连接时，黑客再度传送新一批需要确认的信息，这个过程周而复始，最终导致服务器处于瘫痪状态

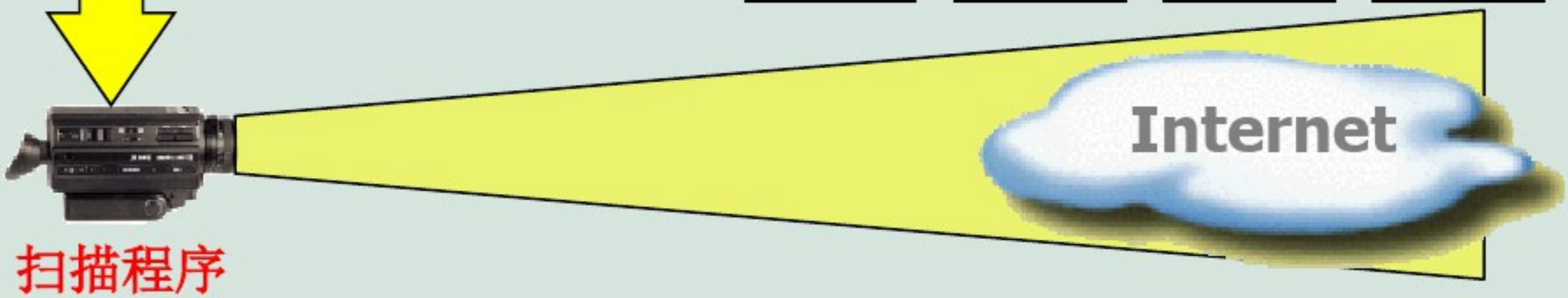
- 很多网络服务程序（如：IIS、Apache等Web服务器）能接受的TCP连接数是有限的，一旦有大量的TCP连接，即便是正常的，也会导致网站访问非常缓慢甚至无法访问，TCP全连接攻击就是通过许多僵尸主机不断地与受害服务器建立大量的TCP连接，直到服务器的内存等资源被耗尽而被拖跨，从而造成拒绝服务，这种攻击的特点是可绕过一般防火墙的防护而达到攻击目的，缺点是需要找很多僵尸主机，并且由于僵尸主机的IP是暴露的，因此容易被追踪。

DDoS攻击过程

黑客

1 黑客利用工具扫描Internet，发现存在漏洞的主机

非安全主机



扫描程序

DDoS攻击过程

黑客

Zombies

2

黑客在非安全主机上安装类似“后门”的代理程序

DDoS攻击过程

黑客

主控主机

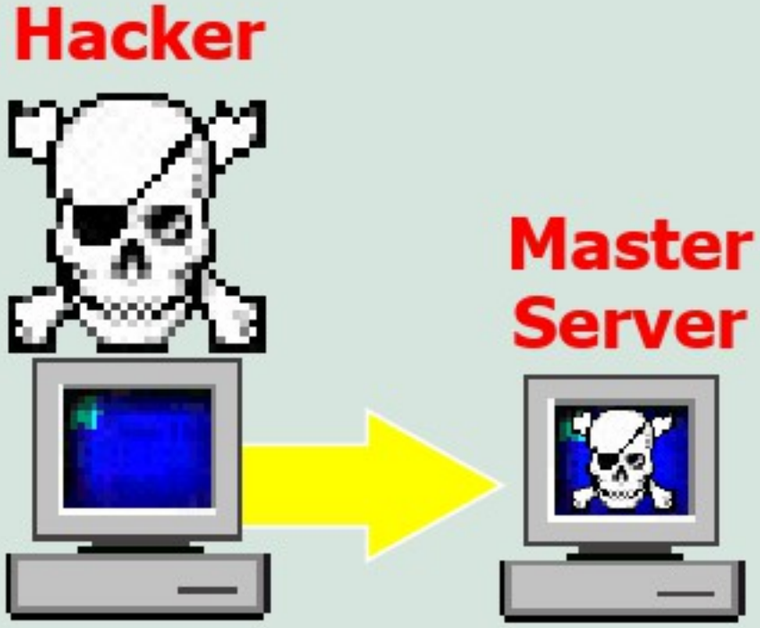
Zombies

Internet

3

黑客选择主控主机，用来向“僵尸”发送命令

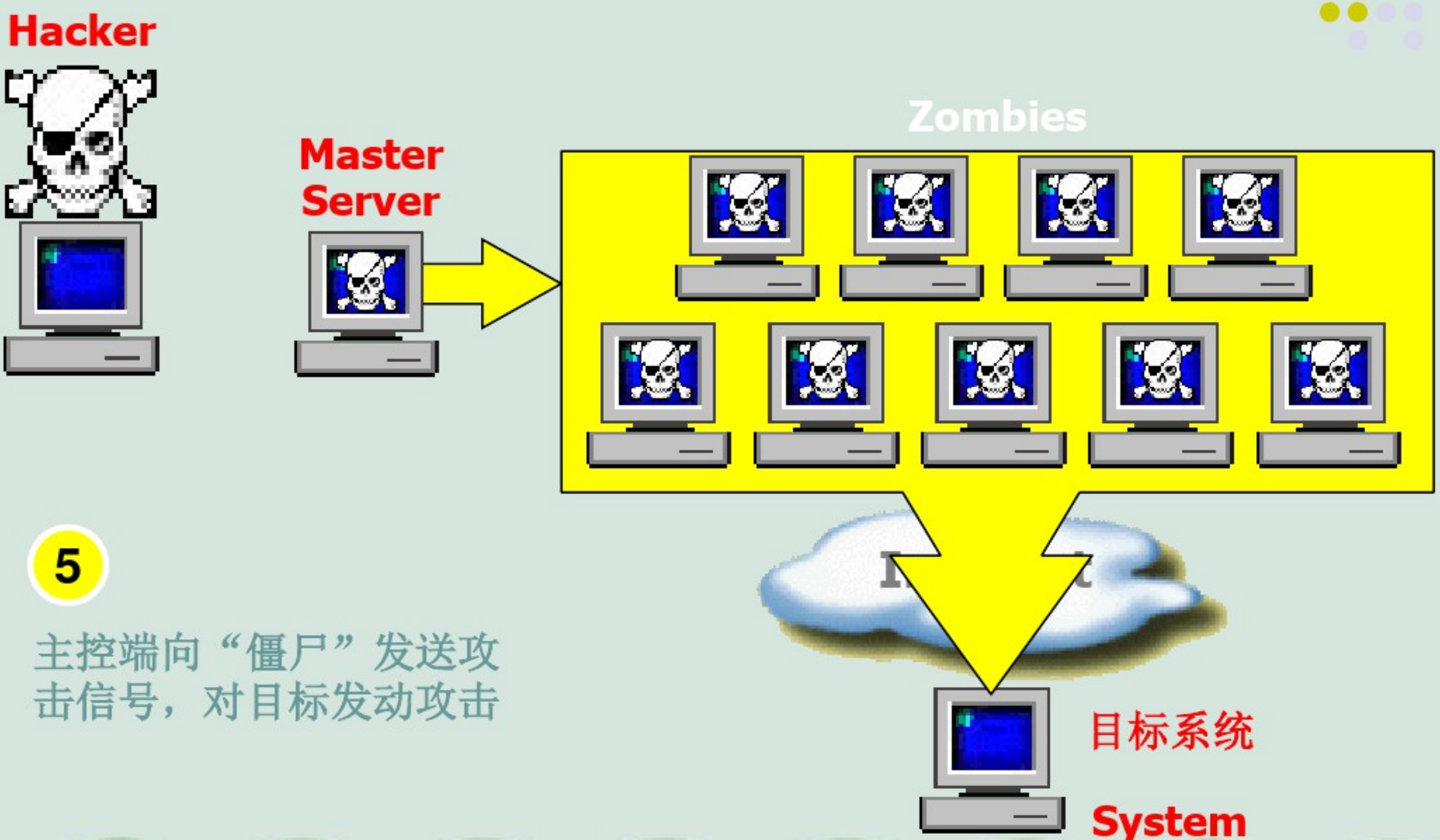
DDoS攻击过程



4

通过客户端程序，黑客发送命令给主控端，并通过主控主机启动“僵尸”程序对目标系统发动攻击

DDoS攻击过程



5

主控端向“僵尸”发送攻击信号，对目标发动攻击

DDoS攻击过程

黑客

主控主机

僵尸

6 目标主机被“淹没”，无法提供正常服务，甚至系统崩溃

合法用户

服务请求被拒绝

目标

分布式拒绝服务攻击

- 分布式拒绝服务攻击（Distributed Denial of Service）是对拒绝服务攻击的发展。
- 攻击者控制大量的攻击源，然后同时向攻击目标发起的一种拒绝服务攻击。海量的信息会使得攻击目标带宽迅速消失殆尽。
- 相对于一般的拒绝服务攻击，分布式拒绝服务攻击有以下两个特点：

分布式拒绝服务攻击特点

- 由于集中了成百上千台机器同时进行攻击，其攻击力是十分巨大的。即使像Yahoo，Sina等应用了可以将负荷分摊到每个服务器的集群服务器（cluster server）技术，也难以抵挡这种攻击。
- 多层攻击网络结构使被攻击主机很难发现攻击者，而且大部分装有主控进程和守护进程的机器的合法用户并不知道自己是整个拒绝服务攻击网络中的一部分，即使被攻击主机监测到也无济于事。

DDoS攻击过程

攻击过程主要有两个步骤：攻占代理主机和向目标发起攻击。具体说来可分为以下几个步骤：

1探测扫描大量主机以寻找可入侵主机；

2入侵有安全漏洞的主机并获取控制权；

3在每台被入侵主机中安装攻击所用的客户进程或守护进程；

4向安装有客户进程的主控端主机发出命令，由它们来控制代理主机上的守护进程进行协同入侵。

DDoS攻击的网络结构

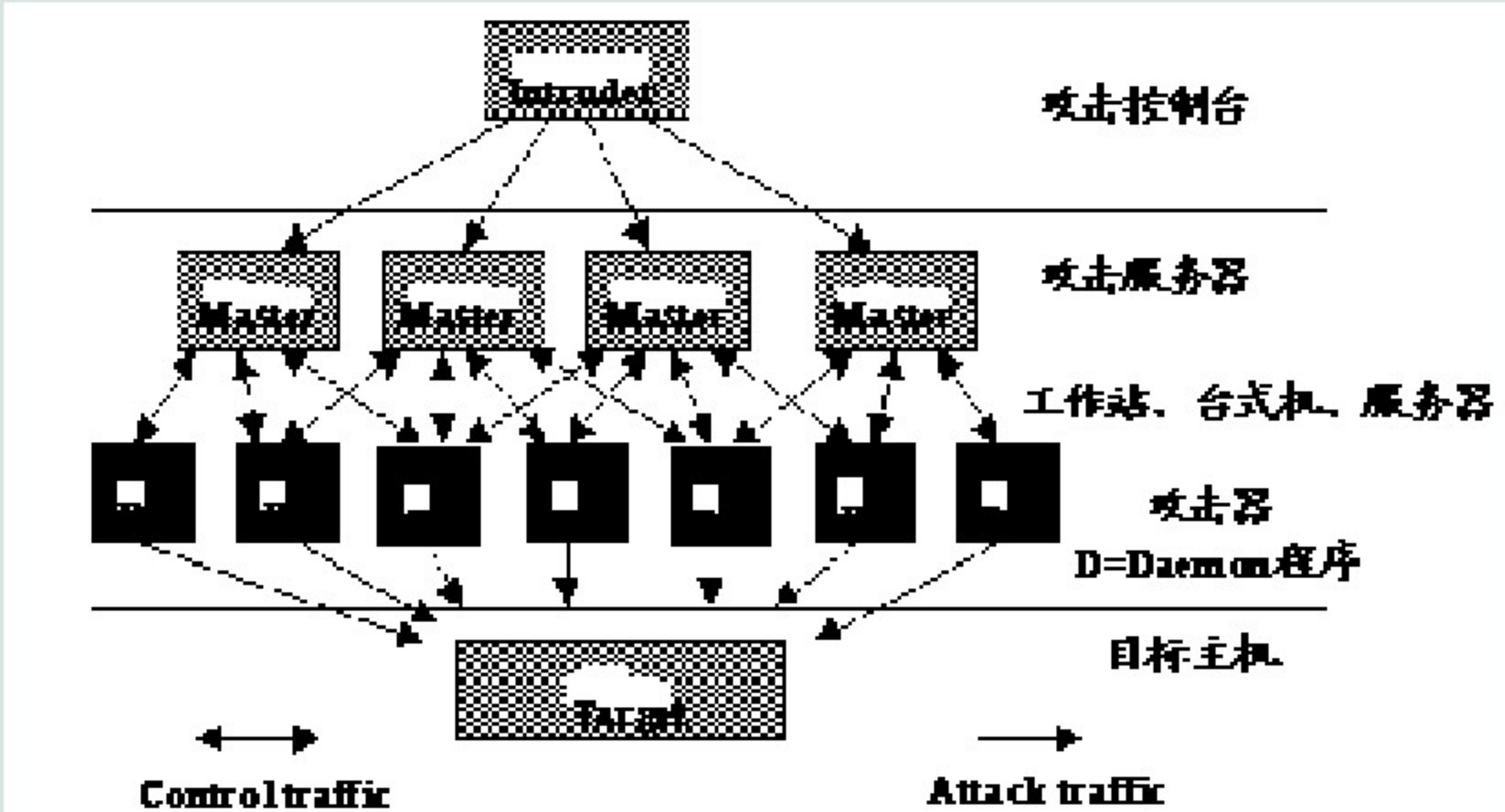


图1 分布式拒绝服务攻击入侵示意图

攻击端： 攻击者在此操纵攻击过程

主控端客户进程： 被攻击者控制的主机，并运行了DDoS主控端程序。

代理端守护进程： 响应主控端攻击命令，向攻击目标发送拒绝服务攻击数据包。

DDOS的表现形式

- 一种为流量攻击，主要是针对网络带宽的攻击，即大量攻击包导致网络带宽被阻塞，合法网络包被虚假的攻击包淹没而无法到达主机；

- 另一种为资源耗尽攻击，主要是针对服务器主机的攻击，即通过大量攻击包导致主机的内存被耗尽或CPU被内核及应用程序占完而造成无法提供网络服务。

DDoS所利用的协议漏洞

1）利用 IP源路由信息的攻击

由于 TCP/ IP体系中对 IP数据包的源地址不进行验证，所以攻击者可以控制其众多代理端用捏造的IP地址发出攻击报文，并指明到达目标站点的传送路由，产生数据包溢出。

2）利用 RIP协议的攻击

RIP是应用最广泛的路由协议，采用 RIP的路由器会定时广播本地路由表到邻接的路由器，以刷新路由信息。通常站点接收到新路由时直接采纳，这使攻击者有机可乘。

DDoS所利用的协议漏洞（续）.

3）利用 ICMP的攻击

绝大多数监视工具不显示ICMP包的数据部分，或不解析ICMP类型字段，所以 ICMP数据包往往能直接通过防火墙。例如，从攻击软件TFN (Tribe flood network)客户端到守护程序端的通讯可直接通过ICMP- ECHOREPLY (Type0)数据包完成。

可直接用于发起攻击的 ICMP报文还有：ICMP重定向报文 (Type5)、ICMP目的站点不可达报文 (Type3)、数据包超时报文 (Type11)。

DDoS攻击的五种常用方式

至今为止，攻击者最常使用的分布式拒绝服务攻击程序主要包括 4种：Trinoo、TFN、TFN2K和Stacheldraht。

1) Trinoo（Tribe Flood Network）攻击

Trinoo是一种用UDP包进行攻击的工具软件。与针对某特定端口的一般UDP flood攻击相比，Trinoo攻击随机指向目标端的各个UDP端口，产生大量ICMP不可到达报文，严重增加目标主机负担并占用带宽，使对目标主机的正常访问无法进行。

DDoS攻击的五种常用方式

2)TFN攻击

TFN是利用ICMP给主控端或分布端下命令，其来源可以做假。它可以发动SYN flood 、UDP flood 、ICMP flood及Smurf(利用多台服务器发出海量数据包，实施DoS攻击)等攻击。

3)TFN2K攻击

TFN2K是TFN的增强版，它增加了许多新功能：

DDoS攻击的五种常用方式

a.单向的对Master的控制通道，Master无法发现Attacker地址。

b.针对脆弱路由器的攻击手段。

c.更强的加密功能，基于Base64编码，AES加密。

d.随机选择目的端口。

4)Stacheldraht攻击

Stacheldraht结合了Trinoo和TFN的特点，

DDoS攻击的五种常用方式

并且它将attacker和master间的通信加密，增加了master端的自动更新功能，即能够自动更新daemon主机列表。

5) SHAFT是一种独立发展起来的DDoS攻击方法，独特之处在于：

首先，在攻击过程中，受控主机之间可以交换对分布端的控制和端口，这使得入侵检测工具难以奏效。

其次，SHAFT采用了“ticket”机制进行攻击，使其攻击命令有一定秘密性。

第三，SHAFT采用了独特的包统计方法使其攻击得以顺利完成。

DDoS攻击新技术——反弹技术

- 反弹技术就是利用反弹服务器实现攻击的技术。
- 所谓反弹服务器（Reflector）是指当收到一个请求数据报后就会产生一个回应数据报的主机。例如，所有的Web服务器、DNS服务器和路由服务器都是反弹服务器。攻击者可以利用这些回应的数据报对目标机器发动DDoS攻击。

反弹技术原理

- 反弹服务器攻击过程和传统的DDoS攻击过程相似，如前面所述的4个步骤中，只是第4步改为：攻击者锁定大量的可以作为反弹服务器的服务器群，攻击命令发出后，代理守护进程向已锁定的反弹服务器群发送大量的欺骗请求数据包，其原地址为受害服务器或目标服务器。

反弹技术实现DDoS攻击与传统DDoS攻击的区别：

1．反弹技术实现DDoS攻击比传统DDoS攻击更加难以抵御。实际上它的攻击网络结构和传统的相比多了第四层——被锁定的反弹服务器层。反弹服务器的数量可以远比驻有守护进程的代理服务器多，故反弹技术可以使攻击时的洪水流量变弱，最终才在目标机汇合为大量的洪水，其攻击规模也比传统DDoS攻击大得多。

2．目标机更难追查到攻击来源。目标机接收到的攻击数据报的源IP是真实的，反弹服务器追查到的数据报源IP是假的。又由于反弹服务器上收发数据报的流量较小（远小于代理服务器发送的数量），所以，服务器根据网络流量来自动检测是否为DDoS攻击源的这种机制将不起作用。

DDoS攻击下的防御

- 对DDoS攻击体系的检测与防范是一个整体行为，必须从主控端、代理端、目标端分别进行。总体上包括两个方面：
  - 一是主控端与代理端主机应防止被攻击者侵入并加以利用。
  - 二是在目标端建立监控机制及时检测网络流量变化判断是否发生DDoS攻击以便采取适当措施。

DDoS的防御(主机上的设置)

几乎所有的主机平台都有抵御DoS的设置，总结一下，基本的有几种：

- a. 关闭不必要的服务
- b. 限制同时打开的Syn半连接数目
- c. 缩短Syn半连接的time out 时间
- d. 及时更新系统补丁