
# 一种基于DDoS活动的僵尸网络检测方法

任文韬 夏震 丁伟
东南大学
2015.11.25

- 研究背景及相关工作
- 僵尸网络检测
- DTS系统设计与实现
- 总结与展望

# 一.　研究背景及相关工作

●分布式拒绝服务(DDoS)攻击是当今互联网的重要威胁之一

●DDoS攻击通常是通过僵尸主机进行的

●DDoS攻击离不开僵尸网络的配合，与僵尸网络关联紧密

在骨干网中

(1)背景流量的干扰

(2)加密技术

(3)控制命令流量较少

等因素的影响，僵尸网络的检测难以有效实施;

DDoS攻击造成

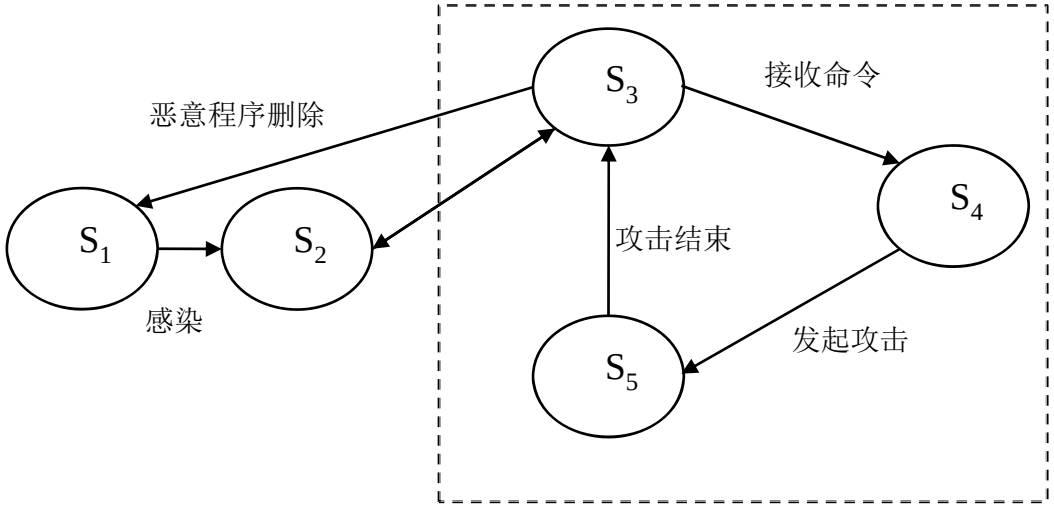
(1)网络流量的大幅度增加

(2)受攻击目标入出流量比大幅度变化

等明显特征，DDoS攻击的检测更易实现

# 二. 僵尸网络检测

DDoS攻击中僵尸主机活动周期




$S_1$：正常网络主机状态

$S_2$：潜伏状态

$S_3$：待命状态

$S_4$：活跃状态

$S_5$：攻击状态

- {S3, S4, S5}构成的循环会被重复使用
- 僵尸主机接受命令后在T时间内发起攻击

如果To时刻检测到攻击，控制命令在(To-T)~ To的所有报文中

DDoS攻击检测需要提供的数据：
三元组<SIP, TargetIP, StartTime>

I. 攻击发起方的地址集:SIP

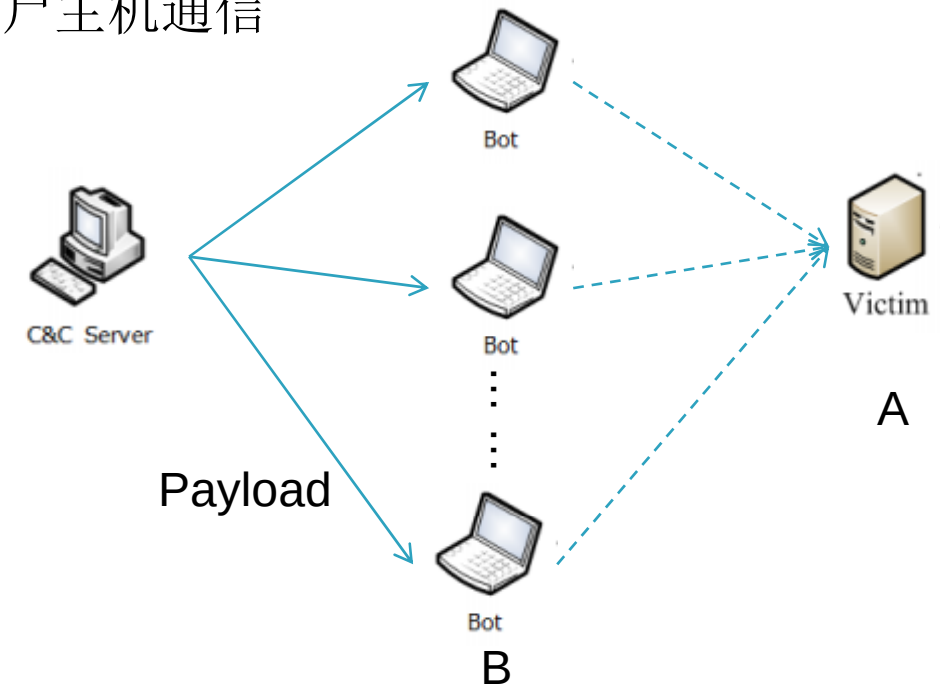
II. 受攻击目标地址:TargetIP

III. 攻击开始的时间:StartTime

原理：C&C在每次攻击前会与僵尸主机通信

明文采用方法一：

C&C Server会将攻击目标的地址发送给僵尸主机，以攻击目标的地址为特征进行匹配。

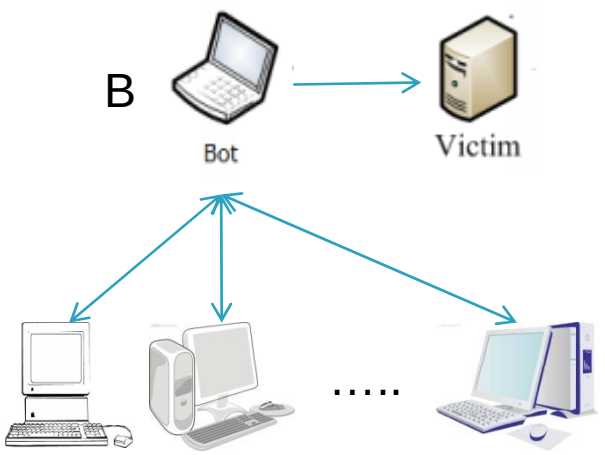


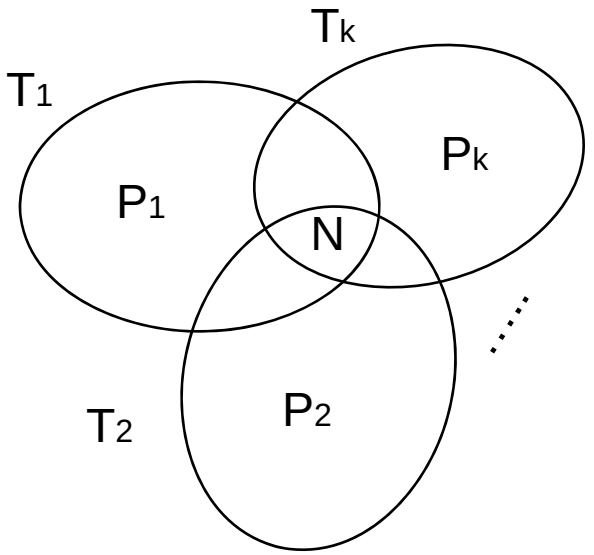
密文采用方法二：

●在B发起攻击前T时间内，对所有与B之间有通信行为的主机建立地址集合P，C&C Server IP被包含在P中

●K次攻击建立集合$P_1$~$P_k$，对$P_1$~$P_k$取交集，结果为N

●如果N的大小为1，则该IP就是僵尸网络的C&C Server；如果N>1，则逐步增大K值



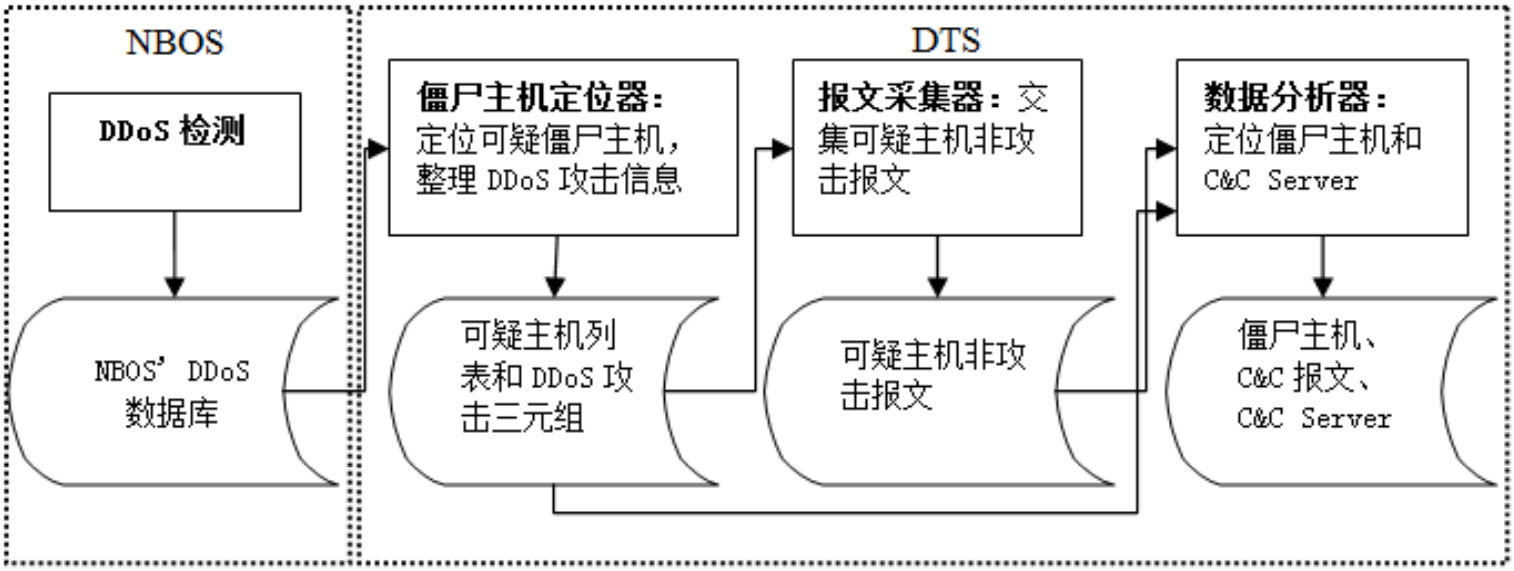



# 三. DTS系统设计与实现

根据之前的理论分析设计实现了一个基于DDoS攻击实现僵尸网络追踪的系统DTS，这个系统可以在DDoS检测系统的支持下实现定位僵尸主机并追踪C&C报文和C&C Server的功能。

DDoS检测功能由一个可以在大规模接入网边界实时检测的网络管理和安全检测系统NBOS提供。

# 工作流程：


NBOS
DDoS 检测
NBOS’ DDoS 数据库
DTS
僵尸主机定位器：定位可疑僵尸主机，整理 DDoS 攻击信息
可疑主机列表和 DDoS 攻击三元组
报文采集器：交集可疑主机非攻击报文
可疑主机非攻击报文
数据分析器：定位僵尸主机和 C&C Server
僵尸主机、C&C 报文、C&C Server

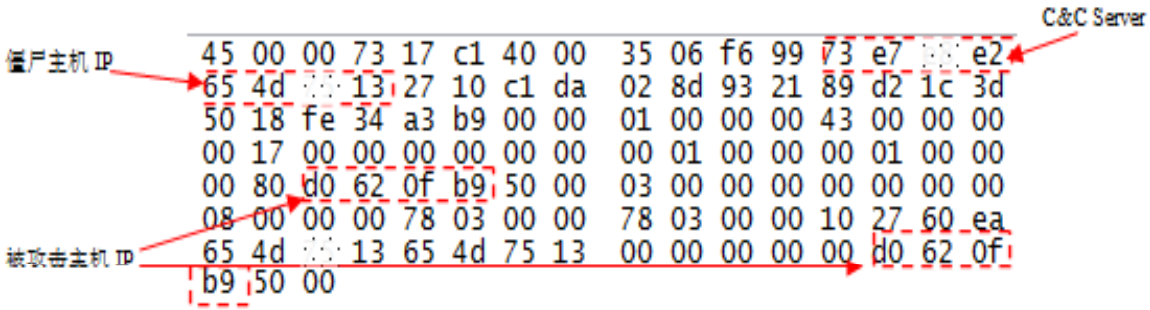
实验结果
实验时间：2015.5.17 -2015.5.21 共计96小时

位置：CERNET 南京主节点的实际网络环境

检测结果：在此期间，根据NBOS提供的DDoS攻击数据以及报文采集器的数据，成功找到8个C&C Server，并获取了相应的C&C报文。

| 僵尸主机 | 采集开始时间 | 初次报文时间 | C&C报文协议 | 检测方法 | C&C server |
|---|---|---|---|---|---|
| 210.29.*.10 | 5-15 13:47:54 | 5-15 15:22:26 | TCP | 1 | 222.186.*.91 |
| 202.195.*.199 | 5-15 15:40:00 | 5-15 15:45:15 | TCP | 2 | 222.23.*.208 |
| 210.29.*.22 | 5-15 15:13:46 | 5-15 15:45:34 | TCP | 1 | 222.186.*.91 |
| 222.192.*.24 | 5-15 15:58:37 | 5-15 16:02:57 | TCP | 1 | 43.240.*.237 |
| 202.119.*.130 | 5-16 07:25:44 | 5-16 07:30:30 | TCP | 1 | 80.242.*.218 |
| 121.248.*.3 | 5-16 03:50:00 | 5-16 10:30:41 | TCP | 1 | 23.234.*.11 |
| 202.119.*.69 | 5-17 04:50:19 | 5-17 04:55:36 | UDP | 1 | - |
| 202.119.*.64 | 5-17 15:01:55 | 5-17 18:08:01 | TCP | 1 | 117.21.*.29 |
| 222.192.*.23 | 5-18 09:27:30 | 5-18 11:58:01 | TCP | 1 | 23.234.*.225 |
| 101.77.*.19 | 5-16 02:19:54 | 5-18 17:37:16 | TCP | 1 | 115.231.*.226 |

| | |
|---|---|
| 僵尸主机 IP： 101.77.*.19 | 教育网　江苏省网某接入单位 |
| C&C Server IP： 115.231.*.226 | 中国大陆某运营商 |
| 被攻击主机IP： 208.98.*.185 | 美国 |
| C&C报文时戳： | 2015.05.18 17:32:17 |
| DDoS攻击开始时间： | 2015.05.18 17:37:16 |
| 检测使用规则： | 规则一 |



# 四. 总结与展望

本文就在大流量背景下检测僵尸主机并定位C&C Server的问题提出了一种利用DDoS攻击检测定位可疑僵尸主机，再通过对可疑主机采集报文进行针对性分析的方法。而基于这个思路的试验系统DTS在CERNET南京主节点试验表明，该研究思路具有可行性。

改善目标：

- 系统参数的设定还需要更多的实验来精准设定
- 数据分析方法不够完善


# 谢 谢 ！