僵尸网络

维基百科，自由的百科全书

僵尸网络（Botnet，亦译为丧尸网络、机器人网络）是指骇客利用自己编写的分布式拒绝服务攻击程序将数万个沦陷的机器，即黑客常说的僵尸电脑或肉鸡，组织成一个个控制节点，用来发送伪造包或者是垃圾数据包，使预定攻击目标瘫痪并“拒绝服务”。通常蠕虫病毒也可以被利用组成僵尸网络。

最早的僵尸网络出现在1993年，在IRC聊天网络中出现。1999年后IRC协议的僵尸程序大规模出现。曾有一个新西兰19岁的黑客控制了全球150万台计算机，中国唐山的黑客也控制了6万台中国的计算机对某音乐网站进行分布式拒绝服务（DDoS）攻击，造成该网站不论将服务器转移到台湾还是美国都无法正常提供服务，损失上百万元人民币，河北唐山黑客的僵尸网络规模也是中国目前为止最大的，目前这两位黑客均已被逮捕。[1]

2011年4月13日美国联邦司法部和联邦调查局（FBI）宣布破获大批中毒电脑所组成的“僵尸网络”(botnet)， 已全面关闭名为Coreflood服务器和网络域名，并对13名嫌疑人起诉。该网络运作将近10年，全球有超过200万台个人电脑被Coreflood恶意程序感染。[2]

目录

用途

- 黑客发送命令开“丧尸”的SOCKS代理用来发送垃圾邮件
- 分布式拒绝服务攻击商业竞争对手的网站

等共10种左右的用途

危害程度

有害软件	传播性	可控性	窃密性	危害级别
僵尸网络	具备	高度可控	有	全部控制：高
木马	不具备	可控	有	全部控制：高
间谍软件	一般没有	一般没有	有	信息泄露：中
蠕虫	主动传播	一般没有	一般没有	网络流量：高
病毒	用户干预	一般没有	一般没有	感染文件：中

表格来源[3]

参看

- 风暴僵尸网络
- 脚本小孩（script kids）
- 缓存溢出（Buffer overflow）即可以被蠕虫利用

参考文献

1. ^ CNCERT/CC配合公安部门捣毁一大规模僵尸网络 (http://www.isc.org.cn/20020417/ca290326.htm)：2004年河北唐山黑客许某控制近十万台“僵尸”，其中六万多台在中国境内，包括部分政府和其他部门的计算机
2. ^ 网路执法 关国际僵尸网路. 世界日报. 2011-04-14 [2011-04-18] （中文（台湾））.
3. ^ CNCERT / CC的文献《僵尸网络的威胁和应对》

外部链接

- 法治在线破获“网络僵尸” (http://news.xinhuanet.com/video/2005-05/17/content_2966558.htm)
- 跨省追踪破坏元凶幕后大战电脑"僵尸网络" (http://news.xinhuanet.com/newmedia/2005-05/31/content_3023916.htm)
- “互联网之父”：全球25%电脑为“僵尸” (http://tech.163.com/07/0130/09/362T7SAT00091KUI.html)
- 僵尸网络研究系列文章之一 (http://www.media.edu.cn/wang_luo_an_quan_5177/20060630/t20060630_186389.shtml)