教你防范新型僵尸网络攻击思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E6_95_99_E4_BD_A0_E9_98_B2_E8_c101_644240.htm 僵尸网络是指采用垃圾邮件、恶意程序和钓鱼网站等多种传播手段，将僵尸程序感染给大量主机，从而在控制者和被感染主机之间形成的一个可一对多控制的网络。这些被感染主机深陷其中的时候，又将成为散播病毒和非法侵害的重要途径。如果僵尸网络深入到公司网络或者非法访问机密数据，它们也将对企业造成最严重的危害。 一、僵尸网络的准确定义 僵尸网络是由一些受到病毒感染并通过安装在主机上的恶意软件而形成指令控制的逻辑网络，它并不是物理意义上具有拓扑结构的网络，它具有一定的分布性，随着 bot程序的不断传播而不断有新的僵尸计算机添加到这个网络中来。根据最近的一份调查，网络上有多达10%的电脑受到Bot程序感染而成为僵尸网络的一分子。感染之后，这些主机就无法摆脱bot所有者的控制。 僵尸网络的规模是大还是小，取决于bot程序所感染主机的多寡和僵尸网络的成熟度。通常，一个大型僵尸网络拥有1万个独立主机，而被感染主机的主人通常也不知道自己的电脑通过IRC(Internet Relay Chat)被遥控指挥。 由于Bot程序混合了很多恶意软件技术，准确的描述什么叫bot程序以及bot程序的成熟度是很难的。僵尸网络攻击所采用的技术横跨了传统和新兴的界限，它们常采取的攻击方法有如下一些： 分布式拒绝服务攻击(DDoS)攻击 一般来说，僵尸网络被用来发动DDoS攻击，DDoS攻击的是电脑系统或是可能导致服务中断的网络，最典型的就是通过消耗受害者的网络带宽或是加载过多的

计算资源来使系统崩溃。除此之外，由于DDoS攻击导致每秒发送过多的信息包数量，就会将系统的带宽消耗殆尽。到目前未知，我们所分析的所有的僵尸计算机都极有可能对其它主机发动DDoS攻击。最常用的方式就是TCP SYN和UDPab(User Datagram Protocol, 用户数据报协议)洪水攻击方式。脚本将DDoS是为一种解决一切社会问题的方法。 更进一步的研究表明，僵尸网路甚至会被别有用心者用来发动对竞争对手的DDoS攻击。Operation Cyberslam记录了Jay R. Echouafni 和 Joshua Schichtel(他化名为EMP)的事件。Echouafni在2004年8月25号被控多重罪名导致受保护的计算机受到威胁。他与EMP合作操控一个僵尸网络发送大量的垃圾邮件，并且对垃圾邮件黑名单服务器发动DDoS攻击使之瘫痪。此外，他们针对全球最大的网上计算平台Speedera的DDoS攻击使得这一站点罢工，而这样做的目的只不过是为了打垮一个竞争对手的网站而已。 由于DDoS并不局限于网站服务器，实际上，一切形式的英特网的服务都会沦为他们攻击的对象。通过使用特定形式的攻击，高层次的网络协议可以备用做增加网络负载量的有效工具，譬如说在受害者的网络里的BBS上或是递归HTTP溢出运行无数的搜索请求。所谓递归HTTP溢出是指僵尸计算机的威胁从给定的一个HTTP链接上指向所有网站上的链接，以一种递归的方式出现。这也叫做蜘蛛网般的攻击。 间谍和恶意软件 僵尸网络比如臭名昭著的Zombies，通常都会在用户不知情的情形下受利益驱动而监视并报告用户的上网行为。它们也会安装一些工具来收集用户的键盘记录和系统漏洞等信息，并将这些信息兜售给第三方。 身份盗窃 僵尸网络还会经常部署一些盗窃用户身份信息、财务信息

或者用户电脑上的密码等信息的工具，然后将这些数据出卖或者直接利用获取利润。 恶意广告软件 Zombies也会根据用户上网习惯自动下载、安装和弹出一些恶意广告，或者强迫用户通过某些网站浏览一些广告。 垃圾邮件 当今的大部分垃圾邮件是由僵尸网络Zombies散发形成的。 网络钓鱼 Zombies可以扫描并确定哪些是有漏洞可以被用来攻击的服务器，通常这些服务器都是合法的而且具有重要机密数据(比如PayPal或者银行站点服务器)，然后窃取服务器上的密码和其他机密数据。 恶意bot程序一直以来都在通过更加隐蔽更加狡猾的方式来感染互联网上的主机。在2007年，僵尸网络成为散发垃圾邮件和发动钓鱼攻击的主要方式。在2008年，僵尸网络所发送的垃圾邮件占整个垃圾邮件数量的90%。而在2009年，垃圾邮件则直接通过P2P方式四处传播。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com