各种各样的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__E5_90_84_E7_A7_8D_E5_90_84_E6_c101_644303.htm 我们在应对僵尸网络攻击的时候，首先套做的就是了解什么是所谓的僵尸网络。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。 二、新型僵尸网络的特点 2009年，一些主要的僵尸网络在互联网上都变得更加令人难以琢磨，以更加不可预测的新特点来威胁网络安全。僵尸网络操纵地点也比以前分布更广。它们采用新技术提高僵尸网络的的运行效率和灵活机动性。很多合法网站被僵尸网络侵害，从而影响到一些企业的核

心竞争力。 最新型的僵尸网络攻击往往采用hypervisor技术。hypervisor技术是一种可以在一个硬件主机上模拟躲过操作系统的程序化工具。 hypervisor可以分别控制不同主机上的处理器和系统资源。而每个操作系统都会显示主机的处理器和系统资源，但是却并不会显示主机是否被恶意服务器或者其他主机所控制。 僵尸网络攻击所采用的另外一种技术就是Fast Flux domains。这种技术是借代理更改IP地址来隐藏真正的垃圾邮件和恶意软件发送源所在地。这种技术利用了一种新的思想：被攻陷的计算机仅仅被用来当作前线的代理，而真正发号施令的主控计算机确藏在代理的后面。安全专家只能跟踪到被攻陷代理主机的IP地址，真正窃取数据的计算机在其他地方。代理主机没有日志、没有相关数据、没有文档记录可以显示攻击者的任何信息。最为精巧的地方在域名服务这部分，一些公司为了负载平衡和适应性，会动态地改变域名所对应的IP地址，攻击者借用该技术，也会动态地修改Fast-Flux网络的IP地址。 而最为众人所知的技术莫过于P2P了。比如，Nugache僵尸网络就是通过广泛使用的IM工具点对点来实现扩充，然后使用加密代码来遥控指挥被感染主机。那也就意味着这种方式更加令人难以探测到。而且僵尸网络也比较倾向使用P2P文件共享来消除自己的踪迹。 无论是使用Fast Flux、P2P还是hypervisor技术，僵尸网络所使用的攻击类型都比以前变得更加复杂多样。显然，僵尸网络威胁一直在不断地增长，而且所使用的攻击技术越来越先进。这就需要我们使用更加强大的安全防护工具来保护个人和公司网络的安全。 三、僵尸网络的危害 随着僵尸网络的不断渗透和扩散，公司必须比以往更加重视和了解边界安全。为此，公

司不仅需要了解僵尸网络的功能和运行机制，也需要了解它们所带来的安全威胁。 对僵尸网络非法入侵做出快速有效的响应，对企业来说可能是一项最为紧迫的挑战。不幸的是，光靠利用基于签名的技术来消除这些安全威胁是远远不够的。使用这种技术往往会花费数小时甚至是数天时间，才能检测到僵尸网络并对其做出响应。僵尸网络最容易吸引各类高科技网络犯罪分子，他们可以借助僵尸网络的温床酝酿和实施各种网络攻击和其他非法活动。 僵尸网络的所有者会利用僵尸网络的影响力对企业展开有针对性的攻击。除了分布式垃圾邮件和攻击电子邮件数据库之外，他们还会发动分布式拒绝服务攻击。僵尸网络越来越喜欢利用窃取企业财务信息或者商业机密，进而对企业进行敲诈勒索和追逐其他利益活动。另外，他们还可以利用企业与企业之间的网络互联或者其他同行合作伙伴来扩大攻击。这也就是为什么企业已经成为僵尸网络重点攻击的受害群体之一的重要原因。 当僵尸网络获得访问公司网络的权限之后，它们就可以肆意捕捉和偷窃公司客户的银行卡、交易和其他重要数据。这样一来，不仅严重危害了客户的私人利益，也损害了公司的宝贵资源和企业形象，从而对企业造成致命创伤。 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