第三篇：僵尸网络追踪及监测研究进展

诸葛建伟

引言

僵尸网络(botnet)是在网络蠕虫、特洛伊木马、后门工具等传统恶意代码形态基础上发展融合而产生的一种新型攻击方式，利用僵尸网络，攻击者可以轻易地控制成千上万台主机对互联网上任意站点发起分布式拒绝服务攻击，发送大量垃圾邮件，从受控主机上窃取敏感信息以牟取经济利益。由于为攻击者提供了隐匿、灵活、高效的一对多控制机制，僵尸网络逐渐得到网络攻击者的青睐，从而已经成为互联网最为严重的安全威胁之一。

据赛门铁客公司 2006 年监测数据表明，我国被僵尸网络控制的主机数占全世界总数的比例从上半年的 20%增长到下半年的 26%，已超过美国成为最大的僵尸网络受害国。

为了探索有效的僵尸网络监测和反制技术手段，狩猎女神项目组从 2005 年即开始着手于僵尸网络追踪及监测技术的研究，并承担了国家 242 信息安全计划项目－“基于蜜网技术的僵尸网络监测系统研究”的研发任务，研究并构建了一套完全自动化的僵尸网络监测系统，能够有效地发现互联网上活跃的僵尸网络，并对其进行长期持续地追踪和监测，该系统在 CNCERT/CC 得到了实际应用。在此基础上，狩猎女神项目组得到国家 242 信息安全计划的滚动资助，将进一步对 HTTP、P2P 等新型僵尸网络的监测技术进行研究和应用。

僵尸网络的发展

僵尸网络的历史渊源可追溯到 1993 年互联网初期在 IRC 聊天网络中出现的 Bot 工具－Eggdrop，它实现为 IRC 聊天网络中的智能程序，能够自动地执行如防止频道被滥用、管理权限、记录频道事件等一系列功能，从而帮助 IRC 网络管理员更方便地管理这些聊天网络。

而之后黑客受到良性 Bot 工具的启发，开始编写恶意僵尸程序对大量的受害主机进行控制，以利用这些主机资源达到恶意目的。1999 年 6 月在互联网上出现的 PrettyPark 首次使用了 IRC 协议构建命令与控制信道，从而成为第一个恶意僵尸程序。之后， IRC 僵尸程序层出不穷，如在 mIRC 客户端程序上通过脚本实现的 GT-Bot、开源发布并广泛流传的 SDbot，具有高度模块化设计的 Agobot 等，这使得 IRC 成为构建僵尸网络命令与控制信道的主流协议。为了让僵尸网络更具隐蔽性和韧性，黑客界不断地对僵尸网络组织形式进行创新和发展，出现了基于 P2P 协议及 HTTP 协议构建命令与控制信道的僵尸程序，著名的案例包括传播后通过构建 P2P 网络支持 DDoS 攻击的 Slapper、使用随机扫描策略寻找邻居节点的 Sinit、基于 WASTE 协议构建控制信道的 Phatbot 以及 2004 年 5 月出现的基于 HTTP 协议构建控制信道的 Bobax 等。

表 1 僵尸程序的演化过程

时间	僵尸程序	作者(或网名)	描述
1993 年 12 月	Eggdrop	Robey Pointer, Jeff Fisher, et, al.	第一个良性 Bot 工具

1999 年 6 月	PrettyPark	不详	第一个以 IRC 构建控制协议的恶意僵尸程序
2000 年	GT-Bot	Sony, mSg and DeadKode	第一个广泛传播的 IRC 僵尸程序
2002 年 2 月	SDbot	SD	第一个开源发布的独立僵尸程序源码基
2002 年 9 月	Slapper	不详	第一个以 P2P 构建通讯协议的蠕虫
2002 年 10 月	Agobot	Ago	高度模块化设计，具有良好的可扩展性和灵活性
2003 年 9 月	Sinit	不详	使用所及扫描策略寻找邻居节点的 P2P 僵尸程序
2004 年 3 月	Phatbot	Ago	基于 WASTE 协议构建的 P2P 僵尸程序
2004 年 5 月	Bobax	不详	第一个使用 HTTP 协议构建控制协议的僵尸程序

僵尸网络的工作机理

传统 IRC 僵尸网络的工作机理如图 1 所示：①攻击者通过各种传播方式使得目标主机感染僵尸程序；②僵尸程序将以特定格式随机产生的用户名和昵称尝试加入指定的 IRC 命令与控制服务器；③攻击者普遍使用动态域名服务将僵尸程序连接的域名映射到他所控制的多台 IRC 服务器上，从而避免由于单一服务器被摧毁后导致整个僵尸网络不可用的情况；④僵尸程序加入到攻击者私有的 IRC 命令与控制信道中；⑤加入信道的大量僵尸程序监听控制指令；⑥攻击者登陆并加入到 IRC 命令与控制信道中，通过认证后，向僵尸网络发出信息窃取、僵尸主机控制和攻击指令；⑦僵尸程序接受指令，并调用对应模块执行指令，从而完成攻击者的攻击目标。

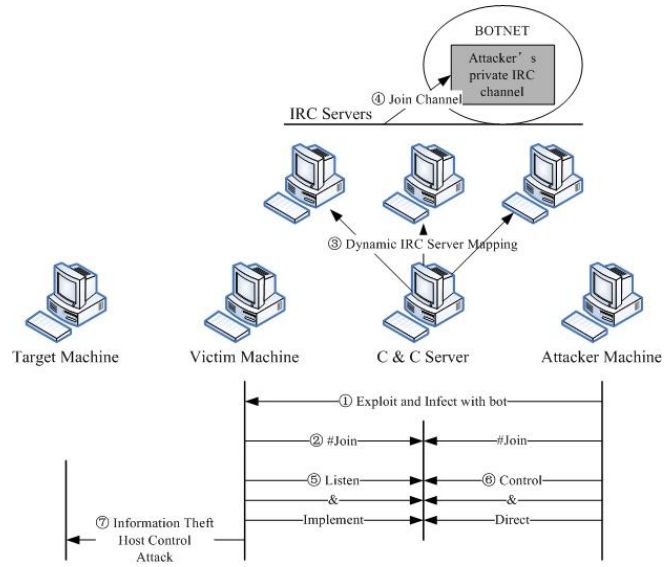

图 1 IRC 僵尸网络的工作机理

IRC 僵尸网络中发送的命令可以按照僵尸程序对应实现的功能模块分为僵尸网络控制命令、扩散传播命令、信息窃取命令、主机控制命令和下载与更新命令，其中主机控制命令还可以细分为发动 DDoS 攻击、架设服务、发送垃圾邮件、点击欺诈等。一条典型的僵尸网络命令如“.advscan asn1smb 200 5 0 -r -a -s”，其中最先出现的点号称为命令前缀，“advscan”则为命令字，表示进行扩散传播，扩散传播命令的参数一般包括远程攻击的漏洞名、使用的线程数量、攻击持续时间、是否报告结果等。僵尸程序在接受此命令后将会按照命令进行扩散传播，并使得被感染的新僵尸主机加入到僵尸网络中，从而扩大僵尸网络的规模。在僵尸网络规模达到一定规模后，攻击者将会利用其控制的僵尸网络达成某些攻击目的，如控制大

量僵尸主机对指定主机进行分布式拒绝服务攻击，如“.ddos syn 215.19.58.xxx 21 200”命令即是对 215.19.58.xxx 上开放的 FTP 服务进行 200 秒 Syn Flood 攻击使其不可访问。

HTTP 和 P2P 僵尸网络的工作机理与传统 IRC 僵尸网络类似，主要的差异在于命令与控制机制的不同。

僵尸网络监测技术及结果

充分了解僵尸网络的内部工作机理是防御者应对僵尸网络安全威胁的前提条件，僵尸网络追踪与监测为防御者提供了一套可行的方法，其基本思想是首先通过各种途径获取互联网上实际存在的僵尸网络相关信息，然后模拟成受控的僵尸程序加入僵尸网络中，从而对僵尸网络的内部活动及规模发展进行跟踪观察和监测。

狩猎女神项目组在承担的 2005 年国家 242 信息安全计划项目“基于蜜网技术的僵尸网络监测系统研究”中构建了一套完整的僵尸网络追踪和监测技术方案，并实现了全自动化的僵尸网络监测系统，其中包括恶意代码样本采集、恶意代码样本分析和僵尸网络追踪三个主要环节。在恶意代码样本采集环节中，通过在全国范围部署 Matrix 分布式蜜网系统，并结合低交互式蜜罐和高交互式蜜罐技术，能够对互联网上实际传播的僵尸程序样本进行有效地捕获；在恶意代码样本分析环节中，实现了基于轻量级沙箱技术和 API 劫持技术的恶意代码自动分析平台，能够高效地对捕获的大量恶意代码样本进行动态分析，对其中的僵尸程序，可自动地对其连接的僵尸网络控制信道信息进行识别和提取，从而发现互联网上实际活动的僵尸网络；在僵尸网络追踪环节，我们基于客户端蜜罐的思想，研发实现了 HoneyBot 僵尸网络追踪软件，该软件能够伪装成为受控僵尸，潜伏进入僵尸网络，并对僵尸网络内部活动和规模发展进行长期持续地追踪和监测。

目前该系统已经在 CNCERT/CC 得到实际应用，从 2006 年 6 月份上线，已投入实际运行超过 1 年时间，系统在一年时间内累计捕获了近 100 万次，9 万多个不同的恶意代码样本，并从中监测了超过 4,000 个活跃的僵尸网络，及被僵尸网络所控制的 150 余万个受控主机 IP 地址，通过长期持续监测，获得了大量宝贵数据，为深入理解僵尸网络行为机理和掌握其发展趋势提供了必要基础。系统在第一时间捕获和分析了黛蛇、Mocbot 等恶意代码，帮助 CNCERT/CC 及时抑制了这些恶意代码的大规模爆发，取得了良好的应用效果。

僵尸网络活动监测统计结果

基于僵尸网络监测系统获取的实际数据，我们对 IRC 僵尸网络的分布特征和活动机理进行了分析，给出了一系列能够在一定程度上反映 IRC 僵尸网络现象的统计结果。

监测到的僵尸网络控制点主要分布于北美、欧洲和东亚，从国家/地区分布的统计情况来看，美国以 37.03%居首位，中国以 7.78%居第二，第三位的是韩国 7.44%，之后的包括荷兰、德国、加拿大、瑞典和英国等欧美发达国家。

僵尸网络控制服务器仍使用 IRC 标准的 6667 端口所占比例已经下降到了 31.49%，大部分攻击者将控制服务器部署在非标准端口，同时也通过使用如 8080、135 等其他应用协议端口以逃过基于端口的网络监测。

僵尸网络控制服务器普遍使用 Unreal 软件（黑客界最为知名的开源 IRC 服务器端软件）搭建，所占比例达到 62.59%，其他搭建软件还包括 u2、bahamut、hybrid 等，但所占的比例都远小于 Unreal。

僵尸网络控制点地域分布

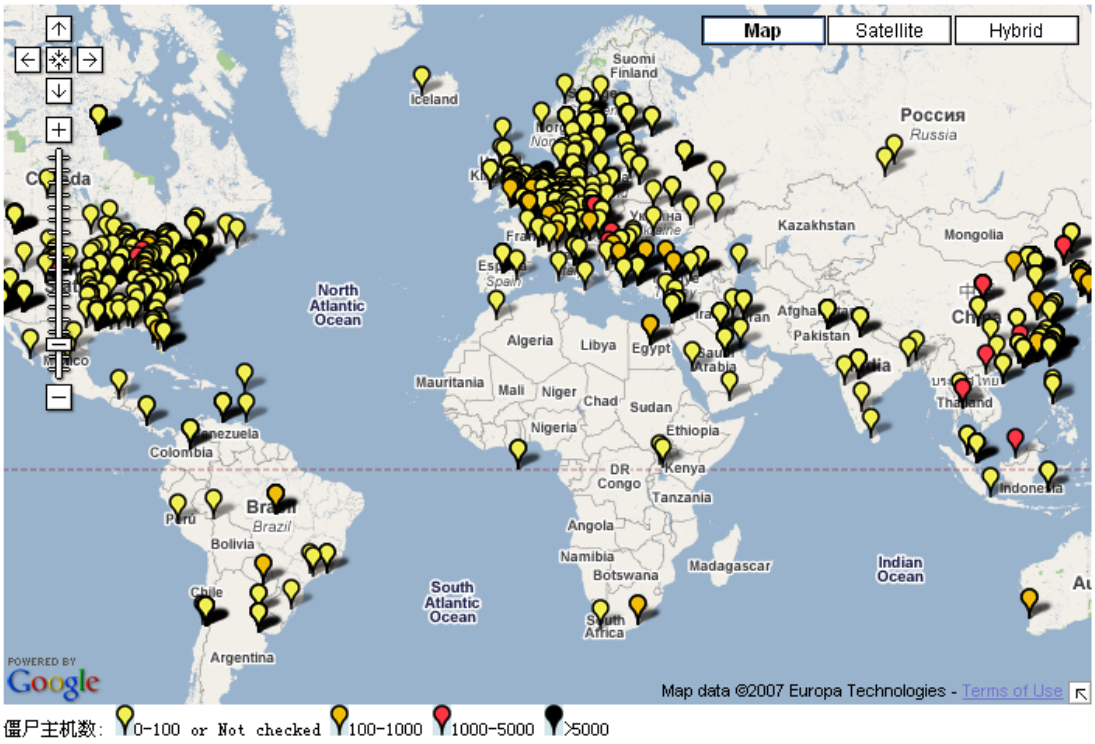

图 2 僵尸网络监测系统发现的僵尸网络控制点的地域分布图

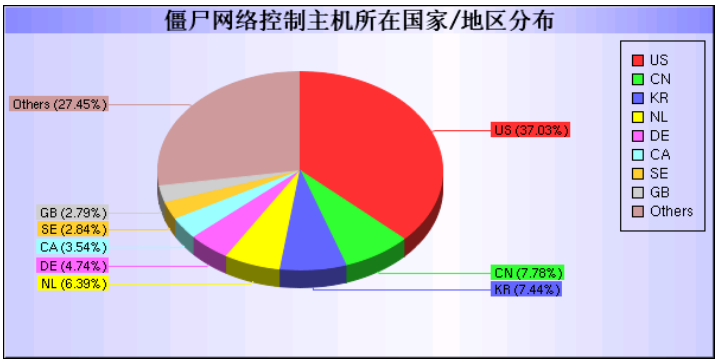

图 3 僵尸网络控制主机所在国家/地区分布

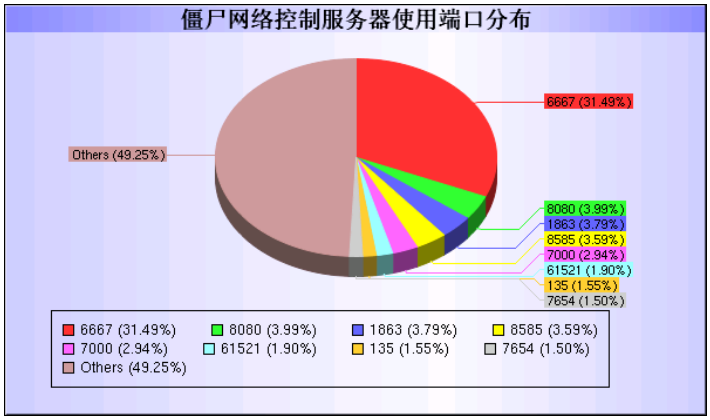

图 4 僵尸网络控制服务器使用端口分布

僵尸网络的规模则呈现小型化趋势，规模在 500 以下的小型僵尸网络占了目前实际僵尸网络中的绝大部分，小型化僵尸网络不易引起计算机安全应急响应部门的注意，但

其控制的资源依然能够对互联网造成严重的分布式拒绝服务攻击威胁。僵尸网络的平均生存周期则达到了 54 天，许多僵尸网络能够持续运行几个月甚至更长时间，这也验证了僵尸网络为攻击者提供了一种隐蔽和鲁棒的一对多控制机制。

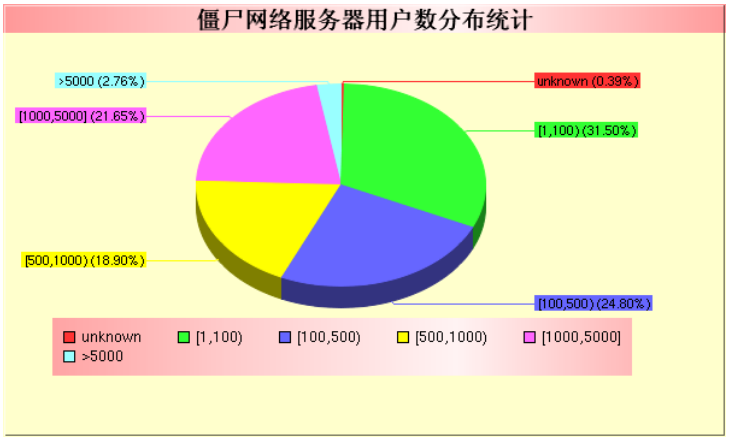

图 5 僵尸网络控制服务器用户数分布统计

根据我们的监测数据统计，亚洲国家/地区被这些僵尸网络控制的僵尸主机数位居前列，由于我们是从中国公共互联网上捕获并发现的这些僵尸网络，而这可以解释为僵尸网络的传播一般具有本地优先的特性，因此具有较强的地域性分布特点，而前 10 位中包括了巴西、中国、马来西亚、泰国、埃及、墨西哥等发展中国家，这在一定程度上说明了发展中国家的互联网安全状况还落后于欧美发达国家，更容易遭受僵尸网络的攻击和危害。从一个典型僵尸网络所控制僵尸主机的地域分布来看，僵尸网络是个全球性问题，即使只是一个僵尸网络案例，其控制的主机也分布于全球几十个，甚至于上百个国家。

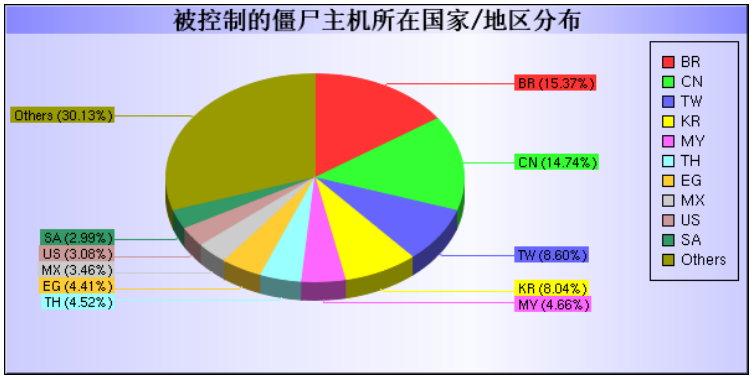

图 6 受控僵尸主机所在国家/地区分布

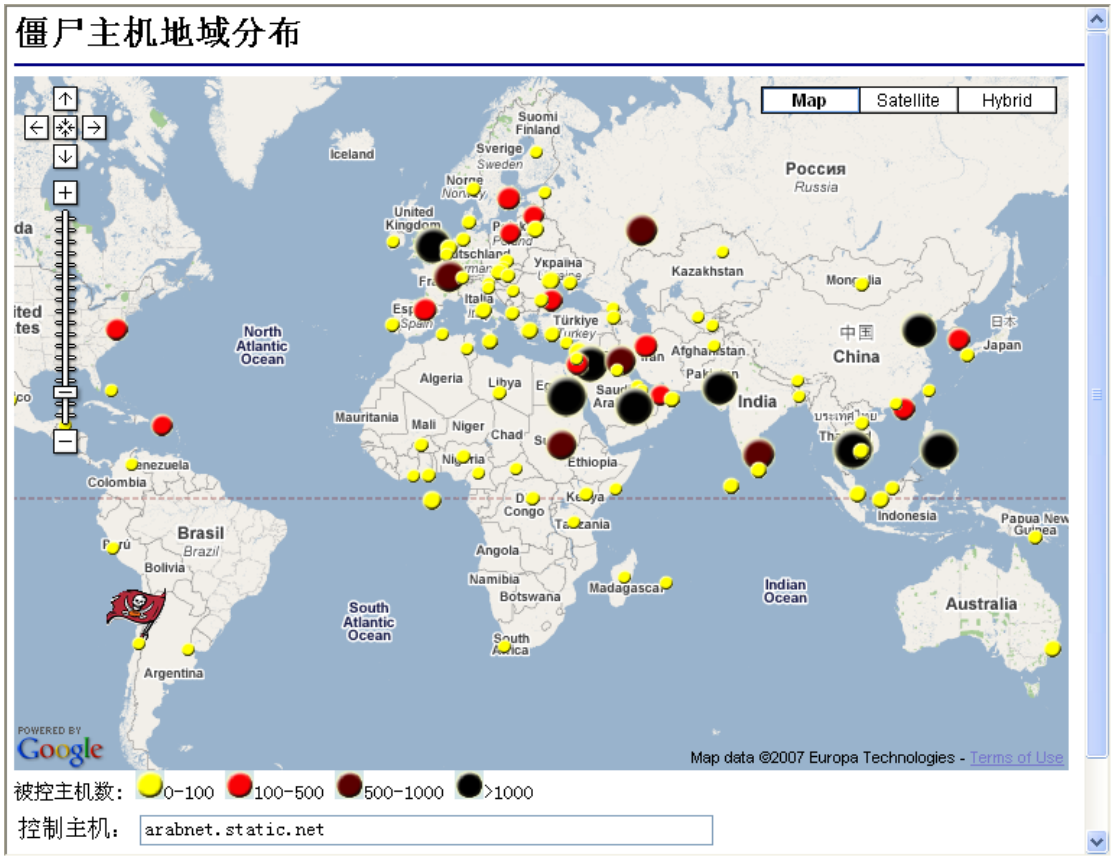

图 7 一个典型僵尸网络所控制的僵尸主机的地域分布图

背后的黑色经济产业链&结束语

僵尸网络之所以在互联网上如此猖獗，其根本原因是其背后拥有一个完善的黑色经济产业链在支撑。

产业链的顶端是一些以编写和出售僵尸程序、盗号木马等计算机病毒牟利的病毒编写者。而产业链的中坚是大量的僵尸网络运营和攻击“黑客”，他们从病毒编写者购买各种病毒，构建僵尸网络攻击平台，并利用这个攻击平台，从互联网上获取更多的受控僵尸主机，而这些受控主机也被称为“傀儡机”或“肉鸡”，捕获的过程被行内形象地称为“抓鸡”。攻击者捕获的“肉鸡”资源可以直接在地下黑市中出售，以换取实际的经济利益，在某知名网站的一个偏僻角落中公然进行着“肉鸡”的买卖，其价格根据所在地、数量的不同从几分钱卖到几块钱一只。在控制如此众多的“肉鸡”资源基础上，攻击者还会在“肉鸡”上安装盗号木马病毒（行内称为“箱子”），盗取 QQ 以及各种网游帐号密码进行出售，这些帐号密码在行内被称为“信封”，这些“信封”也在地下黑市进行公然叫卖，价格也从 QQ 信封最便宜的几分钱到网游信封的十几元不等。

在这条严密的产业链中，还有一些完全无需任何技术的专职盗号人员参与进来，购买大量的“信封”，进行“洗信”从中筛选出 QQ 靓号、QQ 币、网游装备等网络虚拟资产，出售给产业链终端的 QQ 及网游迷恋玩家，而 QQ 靓号、网游装备的价格则在数十元至几百上千元不等。

这条黑色经济产业链已经存在很长时间，虽然今年的“熊猫烧香”案告破和犯罪嫌疑人被捕向人们更加深入地揭示病毒产业链的内幕，也给仍然从事这一黑色产业的“黑客”们敲

响了警钟，但完全消除这一产业链还是任重道远，需要国家法律执行部门、安全应急响应部门、反病毒厂商、安全研究人员以及普通的互联网用户一起群策群力，引导互联网用户提高安全防护水平，一方面通过即时升级补丁程序和病毒特征库从根源上消除被僵尸网络控制的可能，切断黑色产业链的“生产”环节，另一方面加强网络监测和监管力度，通过监控地下黑市交易切断产业链的“销售”环节，并抓取几个较具影响力的典型案件进行处理，以加大对犯罪分子的威慑。双管齐下，相信我们在不远的将来能够还互联网一个明朗的天空。