软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(1):82−96 [doi: 10.3724/SP.J.1001.2012.04101]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

僵尸网络机理与防御技术*

江 健[1], 诸葛建伟[2+], 段海新[2], 吴建平[2]

[1](清华大学 计算机科学与技术系,北京 100084)

[2](清华大学 信息网络工程研究中心,北京 100084)

Research on Botnet Mechanisms and Defenses

JIANG Jian[1], ZHUGE Jian-Wei[2+], DUAN Hai-Xin[2], WU Jian-Ping[2]

[1](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

[2](Network Research Center, Tsinghua University, Beijing 100084, China)

+ Corresponding author: E-mail: zhugejw@cernet.edu.cn

Jiang J, Zhuge JW, Duan HX, Wu JP. Research on botnet mechanisms and defenses. *Journal of Software*, 2012,23(1): 82−96. http://www.jos.org.cn/1000-9825/4101.htm

Abstract: Botnets are one of the most serious threats to the Internet. Researchers have done plenty of research and made significant progress. However, botnets keep evolving and have become more and more sophisticated. Due to the underlying security limitation of current system and Internet architecture, and the complexity of botnet itself, how to effectively counter the global threat of botnets is still a very challenging issue. This paper first introduces the evolving of botnet's propagation, attack, command, and control mechanisms. Then the paper summarizes recent advances of botnet defense research and categorizes into five areas: Botnet monitoring, botnet infiltration, analysis of botnet characteristics, botnet detection and botnet disruption. The limitation of current botnet defense techniques, the evolving trend of botnet, and some possible directions for future research are also discussed.

Key words: network security; botnet; command and control; botnet measurement; botnet detection

摘 要: 以僵尸网络为载体的各种网络攻击活动是目前互联网所面临的最为严重的安全威胁之一.虽然近年来这方面的研究取得了显著的进展,但是由于僵尸网络不断演化、越来越复杂和隐蔽以及网络和系统体系结构的限制给检测和防御带来的困难,如何有效应对僵尸网络的威胁仍是一项持续而具有挑战性的课题.首先从僵尸网络的传播、攻击以及命令与控制这 3 个方面介绍了近年来僵尸网络工作机制的发展,然后从监测、工作机制分析、特征分析、检测和主动遏制这 5 个环节对僵尸网络防御方面的研究进行总结和分析,并对目前的防御方法的局限、僵尸网络的发展趋势和进一步的研究方向进行了讨论.

关键词: 网络安全;僵尸网络;命令与控制;僵尸网络测量;僵尸网络检测

中图法分类号: TP393 **文献标识码**: A

僵尸网络(botnet)是由大量被僵尸程序所感染的主机(bot or zombie)受到攻击者(botmaster)所控制而形成

* 基金项目: 国家自然科学基金(61003127); 国家重点基础研究发展计划(973)(2009CB320505)
收稿时间: 2010-10-27; 定稿时间: 2011-06-24; jos 在线出版时间: 2011-09-09
CNKI 网络优先出版时间: 2011-09-08 17:03, http://www.cnki.net/kcms/detail/11.2560.TP.20110908.1703.002.html

的以恶意活动为目的的覆盖网络(overlay network).Botmaster 可以通过控制服务器操控 bot 发起各种类型的网络攻击,如分布式拒绝服务(DDoS)、垃圾邮件(spam)、网络钓鱼(phishing)、点击欺诈(click fraud)以及窃取敏感信息(information theft)等等.

与以往的安全威胁,如病毒、蠕虫等不同,僵尸网络为攻击者提供了一个高度受控的平台.借助这个平台,攻击者可以按需地发动攻击来谋取经济利益.在经济利益的驱动下,攻击者社区逐渐形成了一个庞大的地下经济市场和分工明确的地下产业链[1−4].在此背景下,各种僵尸程序的数量逐年呈指数级增长,各种攻击活动也越来越频繁[5−7].近年来,还出现了一些超大规模的僵尸网络,如 Conficker[8],Mariposa[9]等,其所控制的 bot 数量达到数百万甚至更多,所拥有的攻击能力足以威胁大型 ISP 甚至整个互联网的运行安全.僵尸网络和以其为载体的各种攻击活动已成为目前互联网最为严重的安全威胁之一.

僵尸网络问题的根源在于目前系统和网络体系结构的局限.操作系统和软件的漏洞导致僵尸程序的感染,而 Internet 开放式的端到端通信方式,使得 botmaster 可以比较容易地对 bot 进行控制.从根本上解决僵尸网络的问题需要系统和网络体系结构的改变,而这样的改变在短时间内难以实际部署.由于在现有体系下难以从根本上解决,僵尸网络问题逐渐形成了一种攻防双方持续对抗和竞争的态势(arms race).对于安全社区来说,了解僵尸网络的运行机制并及时跟踪其发展态势,有针对性地进行防御,是目前应对僵尸网络威胁的关键.

从 2005 年以来,僵尸网络一直是安全领域学术研究的热点问题.ACM,USENIX 等协会先后举办的 SRUTI, HotBots,LEET 等学术研讨会均以僵尸网络作为主要议题之一,各顶级安全学术会议也都有较多僵尸网络研究的论文发表.北京大学计算机研究所、CNCERT/CC、哈尔滨工业大学等单位较早开始关注僵尸网络的问题,并先后发表了研究论文[10−12].诸葛建伟等人在文献[13]中描述了僵尸网络的发展历史和功能结构,并对 2007 年以前的研究进展进行了综述.Zhu 等人[14]和 Bailey 等人[15]也分别从不同的角度对僵尸网络的研究进行了概括性总结.

2008 年以来,围绕僵尸网络展开的持续对抗,使得攻防双方的技术都有了较大的发展.攻击者采用了一些新的方法和技术来提高僵尸网络传播与攻击的效率以及自身的安全性.而在防御一方,安全研究者及时地对新的攻击技术和手段进行了研究,并提出了一些新的检测和防御技术与思路.近年来,一些政府组织、研究机构和企业开始尝试联合对一些大规模的僵尸网络进行处置并取得了明显效果.虽然对僵尸网络的研究和工作逐渐深入,但其威胁的总体趋势并没有改变[5−7].体系结构的局限,僵尸程序数量的急剧增长,僵尸网络传播、控制以及攻击方式的复杂隐蔽和多变等等因素,给防御一方带来了很大的困难.如何在攻防竞争中取得优势,从而能够有效地遏制僵尸网络的威胁,仍然是一项艰巨、持续而具有挑战性的研究课题.

本文主要对近年来僵尸网络攻防双方的技术发展进行归纳和总结,以明确僵尸网络问题和相关研究的现状,为进一步的研究工作提供参考.

本文第 1 节从传播、攻击以及命令与控制这 3 个方面介绍僵尸网络自身工作机制的技术发展.第 2 节从安全威胁监测、工作机制分析、特征分析、检测以及主动遏制这 5 个环节对僵尸网络防御方面的研究进展进行总结.第 3 节讨论目前防御方法的局限性、僵尸网络的发展趋势以及可能的进一步研究方向.第 4 节对全文进行总结.

1 僵尸网络工作机制的发展

深入理解僵尸网络的工作机制,是对其进行有效防御的基础.2008 年以来,研究者发现和分析了一系列新的僵尸网络,如 Koobface[16],Conficker[8],Zeus[17],Torpig[18],Mega-D[19],Mariposa[9],Waledac[20,21]等等,对一些已知的僵尸网络,如 Nugache[22],Storm[23−26]等也进行了更为深入的研究.已有的研究结果表明,僵尸网络不仅在协议和拓扑结构上进一步复杂化,而且还采用一些新技术来提高其恶意活动的效率,并增强其自身的安全性.

僵尸网络的活动主要分为传播(propagation)、命令与控制(command and control)、攻击这 3 个阶段,其中,命令与控制是其工作机制的核心部分.本节首先简要总结僵尸网络在传播和攻击方面的变化情况,然后着重对僵尸网络命令与控制机制的发展进行归纳总结.

1.1 僵尸网络的传播机制

僵尸网络主要通过侵入主机植入僵尸程序来构建,其传播方式主要有远程漏洞攻击、弱口令扫描入侵、邮件附件、恶意文档、文件共享等等.早期的 IRC 僵尸网络主要以类似蠕虫的主动扫描结合远程漏洞攻击进行传播[27],这种方式的主要弱点是不够隐蔽,容易被检测到.近年来,僵尸网络逐渐以更为隐蔽的网页挂马(drive-by download)为主要传播方式[28].

近年来,僵尸网络传播还加入了更多社会工程(social engineering)手段,更具有欺骗性.例如,通过对 Storm 的研究发现,botmaster 会根据近期的新闻和热点事件来变换其传播邮件的标题和内容以增加其感染的几率[24];另一种僵尸网络 Koobface 会盗取被感染用户的社交网络账号,冒充被感染用户向其社交网站好友发送带有恶意 URL 的消息进行传播.目前所流行的一些以好友关系为基础的网络应用,如社交网站 facebook,twitter 以及即时通信(instant message)工具,如 QQ,MSN 等,都成为了僵尸网络传播的重要渠道[7].

另外,一个僵尸网络的传播趋势是简单化和自动化.一些僵尸程序,如 Zeus,SpyEye 等等以及一些漏洞扫描和入侵工具被制作成简单易用的套件(crimeware toolkit),并在地下市场销售[29].利用这些工具,一个毫无经验的攻击者也能轻易制造出僵尸程序变种并感染大量主机,这也是目前僵尸网络泛滥的一个重要原因.

1.2 僵尸网络的攻击活动

目前,僵尸网络的攻击活动仍然以常见的分布式拒绝服务、垃圾邮件、网络钓鱼、点击欺诈以及敏感信息窃取等为主,并没有出现新的攻击形式.但随着互联网用户和带宽的发展,僵尸网络的攻击能力也在不断增强.从各安全机构的调查报告中可以看到,各种类型的攻击,尤其是垃圾邮件、网络钓鱼以及分布式拒绝服务,都处于持续的增长中.分布式拒绝服务的最大单次攻击流量已经超过 100GBps,而且还出现了数次僵尸网络攻击致使大型 ISP 大面积服务发生故障的案例[9].

僵尸网络在攻击能力得到持续提升的同时,也呈现出按照不同类型恶意攻击行为的专业化发展趋势,近年来流行的许多僵尸网络实例专门针对它们所实施的特定类型攻击行为进行命令控制机制的设计与优化.例如,专门针对点击广告互联网经济模式进行点击欺诈的 ClickBot.A[30],Fiesta 与 7cy[31]等僵尸网络;引入代理隐藏机制、采用 URL 缩短和 HTTPS 加密以及变更邮件模版等策略以躲避检测的 Rustock,Mega-D,Storm 等各种 spam 僵尸网络[19,25];以及对命令控制信道进行加密并进行在线银行信息窃取的 Zeus 僵尸网络[17]等.

研究表明,僵尸网络的攻击已经开始作为一种服务在地下市场中销售,如大规模的 spam 僵尸网络表现出很明显的租赁行为[20,24].而且地下市场的需求和竞争促使僵尸网络提供更为细致的服务,近期出现的 Waledac 僵尸网络通过其复杂的结构和控制机制能够提供不同质量的垃圾邮件服务[24].此外,有明显的迹象表明,存在一些种子僵尸网络(seed botnets)来为构建其他的僵尸网络和攻击提供诸如恶意程序安装(pay per install)[29]、钓鱼网站停放、恶意域名停放等等服务.

1.3 僵尸网络的命令与控制机制

僵尸网络的命令与控制机制决定了僵尸网络的拓扑结构、通信效率、可扩展性以及是否容易被防守者发现和破坏,是僵尸网络工作机制的核心部分.本节首先对目前已知僵尸网络的拓扑结构和通信协议进行分类,并结合案例介绍各种类型的僵尸网络的特点,然后总结僵尸网络在提高自身安全性方面的一些新的技术.

1.3.1 僵尸网络的拓扑结构及通信协议

早期的僵尸网络主要以集中式的拓扑结构、以 IRC 作为主要的通信协议,后来逐渐出现采用其他结构和通信协议的僵尸网络.我们将目前已知的僵尸网络分为两大类:

(1) 集中式僵尸网络,bot 直接和控制服务器进行通信,bot 之间没有通信行为.

(2) 分布式僵尸网络,除了 bot 和控制服务器之间的通信以外,bot 之间也会发生通信行为.

集中式僵尸网络根据通信协议的不同又可分为 IRC 僵尸网络、HTTP 僵尸网络以及自定义协议僵尸网络.分布式僵尸网络根据拓扑结构不同可进一步分为结构化 P2P 僵尸网络、无结构 P2P 僵尸网络以及层次化僵尸网络这 3 类.表 1 中列出了我们按以上方式对一些僵尸网络所进行的分类示意.

Table 1 Categories of some known botnets

表 1 一些已知僵尸网络的分类

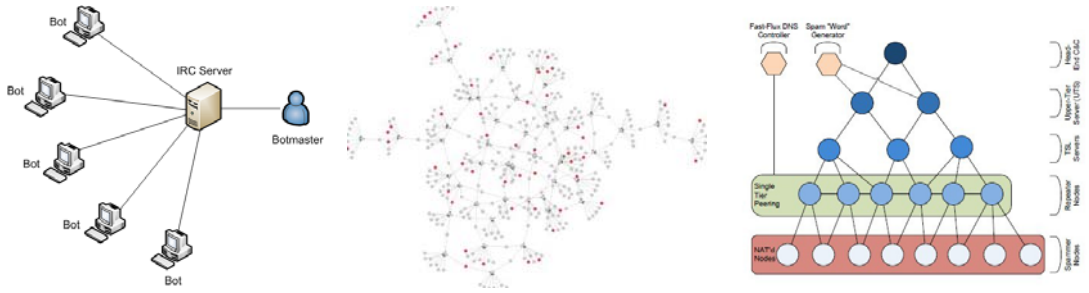
集中式	IRC 僵尸网络	Sdbot, Agobot, GT-Bot, Rbot
	HTTP 僵尸网络	Rustock, Clickbot, Naz, Zeus, Conficker, Torpig
	自定义协议僵尸网络	MegaD, Mariposa
分布式	结构化 P2P 僵尸网络	Phatbot
	无结构 P2P 僵尸网络	Sinit, Nugache
	层次化僵尸网络	Koobface, Storm, Waledac

1.3.1.1 集中式僵尸网络

在集中式僵尸网络中,bot 主要以轮询方式从控制服务器那里获得控制命令.如:在 IRC 僵尸网络中,bot 周期性地加入 IRC 控制频道来获取消息;在 HTTP 僵尸网络中,bot 定期访问控制服务器 URL 来检查是否有控制命令的更新.这类僵尸网络的弱点在于控制服务器容易暴露,但由于其具有结构简单、构建容易、通信效率高的特点,大多数僵尸网络仍然采用这种方式来构建.

- IRC 僵尸网络

早期大多僵尸网络,如 Agobot,GT-bot 等以 IRC 服务作为命令与控制的信道,其典型结构如图 1(a)所示.文献[13]中对 IRC 僵尸网络的发展历史和工作原理进行了详细介绍.IRC 僵尸网络采用已知明文协议,在端口和通信内容等方面具有比较明显的特征;而且 IRC 协议在网络流量中的比例很小,便于监测和分析.虽然 IRC 僵尸网络容易被检测和封锁,但由于其容易构建、控制方便而且实时性好,目前的僵尸网络仍有相当一部分比例使用 IRC 协议作为命令与控制的信道[6].



(a) IRC 僵尸网络 (b) Nugache 僵尸网络[32] (c) Wadelac 僵尸网络[21]

Fig.1 Three different botnet topologies

图 1 3 种不同类型的僵尸网络拓扑结构

- HTTP 僵尸网络

由于 IRC 协议的隐蔽性不好,很多僵尸网络开始使用 HTTP 协议替代 IRC 作为命令与控制方式.相对于 IRC 协议,HTTP 是目前网络应用最主要的通信方式之一,基本不会被屏蔽.而且僵尸网络的通信可以隐藏在大量正常应用流量之中,具有更好的隐蔽性.另外,攻击者还可以很容易地升级到 HTTPS 来加密整个通信过程.采用 HTTP 作为通信协议的僵尸网络有 Conficker,Rustock,Zeus,Torpig 等.此外,少数僵尸网络,如 Naz 等,还直接利用流行的社交网站,如 facebook,twitter 等作为控制服务器,进一步增加了检测和封锁的难度[33].目前,HTTP 已经成为大多数僵尸网络采用的命令与控制协议[6].

- 自定义协议僵尸网络

少数僵尸网络采用自定义的协议进行通信,自定义协议相对更为隐蔽且其通信过程更不容易被研究者所理解.这类僵尸网络的代表有 Mega-D,Mariposa 等.Mariposa 还采用了 UDP 作为传输层协议,相对于 TCP,无连接的 UDP 通信更容易被防火墙等安全设备忽略,使其更加隐蔽.

1.3.1.2 分布式僵尸网络

在集中式僵尸网络中,由于 bot 直接与控制服务器通信,导致控制服务器容易暴露.相比之下,分布式僵尸网

络的控制服务器更加隐蔽,但同时也难以构建和维护,需要攻击者具有比较专业的知识.近年来出现的少数大规模分布式僵尸网络,如 Storm,Waledac 表现出了极其复杂而专业的结构和功能.

- 结构化 P2P 僵尸网络

这类僵尸网络采用了结构化的 P2P 协议.代表性的有采用 WASTE 协议的 Phatbot 以及使用基于 Kademlia 协议的 Overnet 作为命令与控制方式的 Storm 等.虽然结构化 P2P 僵尸网络的控制服务器很难被发现,但 P2P 协议中的查找操作可以获得其他节点的信息,导致 bot 的匿名性较差.研究者利用这个弱点对 Strom 进行了跟踪,在 Overnet 中加入大量的伪装节点将大量的内容发布、搜索和路由请求导向伪装节点以识别出 bot,从而可以估计出整个 Storm 僵尸网络的大小[23].

- 无结构 P2P 僵尸网络

无结构 P2P 僵尸网络的 bot 随机地连接在一起,采用随机转发或洪泛的方式传递控制消息.已知僵尸网络中采用这种结构的有 Sinit 和 Nugache.Sinit 使用随机扫描的方式寻找其他的 bot,而且使用了 UDP 53 端口发送数据包但又不同于 DNS 的报文格式,容易被检测;Nugache 维护了一份可连接的 peer 列表,从列表中随机挑选 peer 尝试连接,连接成功后再相互更新列表.

与结构化 P2P 僵尸网络一样,无结构 P2P 僵尸网络也有 bot 匿名性差的弱点.Dittrich 等人通过不断地连接新的 peer 然后请求更新列表来对整个 Nugache 网络进行了枚举,得到如图 1(b)所示的拓扑图[33].从拓扑中可以看出,Nugache 对 bot 的连接数进行了限制,形成了一个均匀的随机连接的 P2P 网络.

- 层次化僵尸网络

层次化僵尸网络是近年发现的新型僵尸网络.其对 bot 的角色进行区分,利用一些具有公共 IP 地址和在线时间较为稳定的 bot 作为中间层来隐藏真实的控制服务器,同时提供更大的灵活性.这类僵尸网络的代表有 Storm,Waledac,Koobface 等.

Kanich 等人通过对 Storm 的进一步研究发现,Storm 是一个分为 3 层的层次化网络.底层的 worker bots 被用来发送垃圾邮件,worker bots 通过 Overnet 网络来找到 proxy bots,真正的控制服务器 master servers 隐藏在作为代理层的 proxy bots 之后[24].

被认为可能是 Storm 的直接后继的 Waledac 具有比 Storm 更为复杂的结构,如图 1(c)所示,botmaster 以下分为 4 个层次,依次为 UTS,TSL,Repeater 和 Spammer.其中,Spammer 和 Repeater 是被感染的 bot 主机,TSL 和 UTS 是 botmaster 设立的控制服务器.Waledac 使用一种称为 fast-flux[34,35]的技术将 Repeater 作为 Spammer 和 TSL 之间的代理.这种分层代理的技术使 Waledac 在保持隐蔽性和灵活性的同时,不会像 Storm 那样被完全枚举.

早期的 Koobface 是一种集中式僵尸网络,bot 直接和控制服务器进行通信.在被研究机构和 ISP 发现和关停后,Koobface 进行了升级,利用一部分 bot 作为代理节点来隐藏控制服务器,升级后的层次化结构使得 Koobface 的控制服务器很难被发现和关停.

1.3.2 僵尸网络的自身安全性

僵尸网络命令与控制机制的一个重要属性是其自身安全性,一种僵尸网络是否容易被发现和破坏、是否有明显的弱点和漏洞,是攻防双方关注的重点.我们从僵尸网络的隐蔽性和匿名性、加密机制、认证机制、网络发现(bootstrapping)机制这几个方面对僵尸网络的自身安全性进行分析,并介绍相关的技术发展.

1.3.2.1 隐蔽性和匿名性

僵尸网络的隐蔽性和匿名性基本上是由其通信方式所决定的.集中式的僵尸网络 bot 之间的匿名性很好,但控制服务器的隐蔽性很差,很容易暴露.采用 P2P 方式的僵尸网络能够很好地隐藏控制服务器,但由于 P2P 协议的特点,导致 bot 之间的匿名性很差,Storm 和 Nugache 都因为这方面的弱点被研究者枚举出大量的 bot.层次化的僵尸网络能够在保持控制服务器隐蔽性的同时,还能提供较好的匿名性.

1.3.2.2 加密机制

采用明文通信的僵尸网络的行为更容易被分析,而且更容易提取出内容特征串来通过流量内容进行检测.加密机制的采用,在近来发现的僵尸网络中已经比较常见,Zeus,Torpig,Nugache,Mega-D,Waledac 等都采用了简

单或复杂的加密手段.

1.3.2.3 认证机制

认证机制是指 bot 和控制服务器之间是否验证身份、控制消息是否有防止伪造和篡改的机制,这是目前僵尸网络比较薄弱的一个环节.Torpig 的 bot 没有对服务器进行认证,使得研究者能够对其进行劫持而获得大量的数据.Storm 也缺少对控制消息的保护,研究者利用这一点对其控制消息进行篡改,注入自己控制的邮件地址和域名来研究其行为.少数僵尸网络设计了一定的认证机制,Waledac 通过签名和时间戳对其地址更新消息进行了保护,Conficker 也使用了签名来保证其更新不会被假冒.

1.3.2.4 网络发现机制

网络发现机制是指 bot 如何找到控制服务器或者通过其他的 bot 加入到僵尸网络中.对于防御方来说,如果能够找到并切断 bot 和控制服务器之间的联系,就能从根本上关停整个僵尸网络.早期的集中式僵尸网络多采用简单的固定 IP 或者域名的方式来发现控制服务器,P2P 僵尸网络多借助于 P2P 协议的动态发现机制.近年来的攻击者开始采用多个域名或 IP 并结合更新机制来提高僵尸网络的抗关停能力,还发展出了 domain-flux, fast-flux 等新技术.下面我们对僵尸网络的各种网络发现机制及技术进行总结和分析.

- 固定 IP 地址或域名

bot 通过预先设置的静态 IP 地址或者域名来找到控制服务器.这种方式最为简单,多数僵尸网络包括一些较大的僵尸网络,如 Mega-D,Rustock 等仍然使用这种方式.虽然理论上静态的地址和域名容易被追踪和关停,但由于域名或 IP 地址的管理一般跨越网络管理域甚至行政区域,实际操作起来并不容易.一些大规模的僵尸网络设定分布广泛的多个静态 IP 地址或域名,再结合内建的更新机制,由于不同的网络管理域的处置行动很难同步进行,使得这样的僵尸网络具有很好的抗关停能力.

- 随机扫描

bot 通过随机发送数据包来尝试找到其他的 bot 或者控制服务器.这种方式效率低下而且很容易被检测,目前只发现 Sinit 僵尸网络采用了这种机制.

- P2P 动态发现机制

P2P 僵尸网络大多借助于 P2P 网络中的动态发现机制来加入僵尸网络,如 Phatbot 利用 Gnutella 的 cache server 来注册和发现其他的 bot,Storm 和 Nugache 维护动态更新的 peer 列表来加入网络.这种机制不容易被关停,但具有匿名性差的弱点,容易暴露其他的 bot.

- domain-flux

domain-flux 是指 bot 使用某种算法生成大量的域名,然后逐个地对这些域名进行尝试以试图与控制服务器取得联系的一种技术.Conficker,Torpig 等使用了这种技术,使得 botmaster 可以灵活地在多个域名上转移控制服务器.Conficker.C 的域名生成算法每天生成 50 000 个不同的域名,分布在 110 个顶级域.这种技术具有很好的抗关停能力:一方面由于域名数量巨大;另一方面,这些域名跨越多个管理区域,无论是抢注、屏蔽或关停这些域名都很难实行,即使对这些域名的状态进行跟踪也需要耗费大量资源.

- fast-flux

fast-flux 是一种利用 DNS 实现的动态代理技术[34−36].其基本原理是,利用一些具有公共 IP 地址的 bot 作为代理(flux-agent),控制服务器域名被解析为这些 flux-agent 的 IP 地址,真实的服务器隐藏在 flux-agent 背后提供服务.为保持可用性和隐蔽性,与域名关联的 flux-agent 的 IP 地址一直不停地发生变化.fast-flux 又分为 single-flux 和 double-flux 两种类型,关于这两种技术的细节请参考文献[36].

botmaster 使用 fast-flux 技术可以将大量的 bot 形成一个动态的代理网络,使得隐藏在背后的控制服务器很难被发现,僵尸网络的真实结构和工作机制也可以得到隐藏.良好的隐蔽性使得 botmaster 可以长时间使用固定的服务器,而且可以将大量的恶意网站停放在一个服务器上,便于对其资源进行管理.除了僵尸网络控制服务器的域名,fast-flux 网络还被用来解析恶意软件宿主网站、网络钓鱼网站以及其他恶意站点的域名.

1.3.3 僵尸网络命令与控制机制的比较和发展趋势

我们选择 5 种不同时期的僵尸网络,对其命令与控制机制进行比较,表 2 中给出(由拓扑结构和网络发现机制所决定的)从效率和连通性、加密机制、认证机制、隐蔽性以及匿名性这 6 个方面的比较结果.我们对每项属性给出从 0~3 个星号的评价,问号表示未知.从表中可以看出:早期的 IRC 僵尸网络(Rbot)具有很好的效率,但在自身安全性方面较差;后来的僵尸网络明显加强了自身安全性.Torpig 采用的 domain-flux 技术增强了控制服务器的隐蔽性和抵抗关停的能力,但缺少对服务器的认证导致被研究者劫持;Nugache 这种随机连接的网络具有很好的连通性和隐蔽性,主要弱点是匿名性差;Storm 与 Nugache 一样,在匿名性方面有明显的弱点,并且没有对控制消息进行认证和保护;近年出现的 Waledac 在各方面都有针对性的设计,其工作机制已经没有明显的弱点.

Table 2 Comparision of five known botnets's C&C mechanism

表 2 5 种已知僵尸网络命令与控制机制的比较

僵尸程序/网络	效率	自身安全性				
		连通性	加密机制	认证机制	隐蔽性	匿名性
Rbot	★★★	★	—	—	—	—
Torpig	★★★	★★	★★	—	★☆	★★
Nugache	★★	★★★	★★★	?	★★★	★
Storm	★★☆	★★★	★★	★	★★★	★
Waledac	★★☆	★★★	★★☆	★★	★★★	★★

2 僵尸网络防御技术研究进展

对于防御方来说,想要有效地应对僵尸网络的威胁,面临以下几个问题:

(1) 哪些入侵手段和僵尸程序是目前正在广泛流行和传播的,其传播方式、范围及攻击形式是怎样的;

(2) 僵尸网络是如何工作的,采用了什么样的技术;

(3) 僵尸网络的活动具有怎样的特征;

(4) 如何准确地检测出被感染的主机或者已存在的僵尸网络;

(5) 什么样的技术和策略能够有效地遏制僵尸网络的发展.

针对以上问题,安全社区逐渐形成了包括安全威胁监测、工作机制分析、特征分析、在线检测以及主动遏制的整体防御体系.下面我们从这 5 个环节来分别介绍近年来僵尸网络防御技术的研究进展.

2.1 僵尸网络威胁监测

对僵尸网络的活动进行监测,捕获僵尸网络的传播和攻击行为及新的僵尸程序样本,了解僵尸网络的活动范围以及发展态势,是僵尸网络防御体系的第 1 个环节.这方面的工作主要在于研究和开发新的监测技术以及部署覆盖面广泛的监测系统.

蜜罐(honeypot)是对僵尸网络进行监测的最为有效的技术.随着僵尸网络的发展,蜜罐的思想和技术在近几年中得到了很大的发展.针对僵尸网络的多样化传播和攻击方式,研究者也设计实现了各种类型蜜罐,如能够虚拟网络拓扑并模拟各种网络服务的 honeyd[37]、针对服务端溢出漏洞攻击和网络扫描的 nepenthes 以及后续升级版本 dionaea、收集垃圾邮件的 spampots、针对 Web 服务攻击的 Glastopf、能够检测网页是否存在恶意脚本的 Capture-HPC[38]以及 PHoneyC[39],还有专门针对 SSH 服务弱口令扫描的 Kippo 等.另外,还有一些安全监测方面的研究也借鉴了 honeypot 的思想.HoneyBuddy[40]创建和维护陷阱帐号来捕捉即时通信网络中的恶意软件和链接传播,Stringhini 等人在流行的社交网站中设立虚假的 honey-profile 来测量社交网站中 spam 的发送情况[41].

一些安全公司、研究组织和个人以及 CERT 机构在蜜罐的研发以及分布式安全监测系统的部署方面起到了积极的推动作用.国际蜜网项目(the honeynet project)组织引导了大量开源蜜罐的开发工作,并积极推动分布式蜜网的部署工作.Shadowserver 等组织也积极开展了僵尸网络监测的工作,并对一些流行的僵尸程序,如 Conficker, Zeus,SpyEye 等的活动进行了持续的跟踪.国内 CNCERT/CC 也部署了包括蜜网系统的互联网安全监

测平台,并以此为基础定期发布安全报告.教育网应急响应组 CCERT 也正在推进 CERNET 分布式蜜网的部署工作.

2.2 僵尸网络工作机制分析

在通过部署蜜罐或以其他方式获取僵尸程序样本后,研究者通过对僵尸程序样本进行静态分析,并在受控的环境中运行僵尸程序,监控和分析其行为(botnet tracking or botnet infiltration)来揭示其背后僵尸网络的工作机制,整个分析过程可以视为对僵尸程序以及僵尸网络的逆向工程.

由于不同僵尸程序和僵尸网络之间的差异很大,目前这方面的研究主要以人工的个案分析来进行.虽然缺少普适性方法的个案分析缺乏可扩展性,但安全社区仍然在这方面取得了不错的成绩,对新的僵尸网络和技术基本能够及时地发现和揭示,第 1 节中所介绍的各种僵尸网络工作机制多为个案分析后所得到的结果.

以个案分析的方式进行僵尸网络的逆向工程面临可扩展性的问题,无法应对数量庞大的僵尸程序样本.此外,大多数个案分析没有揭示出僵尸网络工作机制背后的经济驱动力.针对这一问题,来自 UCSD 和 UC Berkeley 的研究团队提出了更为自动化、智能化和系统性的僵尸网络跟踪研究计划.这一计划主要包括 3 部分的研究内容:

(1) 安全受控以及可扩展的僵尸程序运行及跟踪平台 Botfarm;

(2) 对僵尸网络命令与控制协议进行完整逆向工程;

(3) 在前面两部分研究的基础上对僵尸网络背后的地下经济体系进行研究.

目前,这项研究计划正在持续开展中,并已在僵尸网络工作机制分析技术和地下经济体系调查等方面取得了丰硕的研究成果.设计实现了用于跟踪僵尸程序的 Botfarm 通用平台,并提出了僵尸网络命令控制协议的形式化模型[42]与自动化逆向工程方法[43].在此基础上,研究者对 Mega-D 僵尸网络进行了深入的分析[19],并通过注入和改变控制命令的方法对 Storm 僵尸网络的价值链进行了分析[24].该计划最近还发表了多篇通过大规模跟踪和测量对垃圾邮件整体经济体系进行分析的论文[44,45],研究结论认为,支付环节是这一地下经济链的瓶颈,并建议采取相应的管理政策来遏制其发展.

2.3 僵尸网络特征分析

对僵尸网络进行监测和跟踪的另一个目的是发现和分析其所具有的一些特征,近年来,这方面的研究主要包括针对 spam 僵尸网络的测量、对特定技术如 fast-flux 的特征分析以及网络流量内容特征提取.

2.3.1 SPAM 僵尸网络测量研究

Kreibich 等人对 Storm 的研究结果表明,Storm 采用了多种技术来逃避垃圾邮件过滤,包括使用词典随机生成内容、大量不同的模板、不停变换垃圾邮件中超链接的域名等等[25].

John 等人构建了一个受控的 spam 僵尸程序运行环境 Botlab[46],通过运行并记录其新发出的垃圾邮件,然后和邮件服务器中原来的垃圾邮件结合进行关联分析用以研究 spam 僵尸网络的行为.其研究结果表明,垃圾邮件的来源集中在几个大的 spam 僵尸网络,而且多个僵尸网络的控制服务器 IP 地址都属于 McColo 这个 ISP.研究者还将 Botlab 中获得的 40 270 个恶意链接在 Google Safe Browsing 黑名单[28]中并进行了测试,发现没有一个包含在黑名单中,这说明 Botlab 这样的测量平台所获得的数据具有更好的实时性.Pitsillidis 等人用类似 Botlab 的方法构建了 Botnet Judo 系统,从而利用僵尸程序发出的垃圾邮件作为样本,更好地对垃圾邮件进行过滤[47].

2.3.2 fast-flux 特征分析

fast-flux 作为一种新的攻击技术引起了研究者的广泛关注,Holz 等人首先对其特征进行研究,并提出了通过域名的 A 记录数、NS 记录数以及域名对应 IP 地址所在的 AS 的数量这 3 项指标结合一定的权重进行计算的指标 flux-score[34].根据这个评判标准,Holz 等人对在 spam 中提取的 7 389 个域名进行了测量,其中,2 197 个域名被认为是 fast-flux 域名,占到 29.7%;而顶级域中,.com,.cn 和.net 的比例占据前三位.Nazario 等人的研究[35]发现,fast-flux 域名的活跃期很短,他们测量的 928 个 fast-flux 域名平均活跃时间为 18.5 天,近三分之一的域名活动不到一个星期.平均每个域名累计对应 2 683 个 IP,最多的一个域名对应了超过 10 万个 IP.Nazario 等人还

对 428 个 fast-flux 域名所关联的 IP 地址进行聚类分析,找出了 26 个不同的 fast-flux 域名停放网络.

2.3.3 僵尸网络流量内容特征的提取

流量内容特征提取对僵尸网络的检测具有非常重要的意义,Rieck 等人在文献[48]中描述了一种自动提取僵尸网络通信的特征内容的方法——Botzilla.他们首先将恶意软件样本在受控的网络环境中重复运行并记录其通信内容,提取出其中的重复出现的内容作为待选特征串,然后通过正常通信内容记录进行筛选得出检测特征串.文献中对 20 种僵尸程序样本进行了实验,其中的 17 种成功生成出了特征串,而且生成的特征串在实验中表现出了很高的准确性,检测率平均达到 94.5%,误报率仅为 0.0001%.

2.4 僵尸网络检测技术

如何准确地检测出被感染的主机或者已存在的僵尸网络,是应对僵尸网络威胁的一个关键问题.僵尸网络检测研究有两个要素:一是数据来源,二是对异常模式的定义.另外,检测方法的准确性、性能以及可部署性也是这方面研究的重要指标.

目前的僵尸网络检测技术采用的数据源主要是网络流量以及一些应用程序的数据(如邮件记录以及 DNS 的日志记录),而对异常模式的定义主要有传统的基于内容特征(signature-based)异常基于特定行为(behavior-based)异常.表 3 从这两个方面总结了近年来的一些新的僵尸网络检测技术,下面我们以分类形式对这些检测技术的方法和特点进行分析.

Table 3 Recently proposed botnet detection techniques

表 3 一些新的僵尸网络检测技术

检测技术	数据源		异常模式		部署位置
	网络流量	应用数据	内容特征	行为特征	
TAMD[49]	√			√	骨干网或者企业网
BotGrep[50]	√			√	骨干网
BotSniffer[52]	√	√	√	√	企业网
BotMiner[53]	√	√		√	企业网
RB-Seeker[54]	√	√		√	企业网
Ref.[55]		√		√	DNS 服务提供商
Ref.[56]		√		√	邮件服务提供商
AutoRE[57]		√	√	√	邮件服务提供商
Botgraph[58]		√		√	邮件服务提供商

2.4.1 基于网络流量内容特征的检测技术

基于内容特征的检测是入侵检测系统的常规检测方法,这种方法适用于已知的具有明确特征的僵尸网络.如早期采用 TCP/8 端口的 Nugache 以及采用 UDP/53 端口的 Sinit.另外,Phatbot,Conficker,Waledac 等的研究报告中也都给出了可直接用于传统入侵检测系统的特征内容.

基于内容特征的检测技术具有准确、快速、容易部署的特点,是目前实际应用最为广泛的检测方法.其局限性在于容易被变形、多态等技术所逃避,对未知的僵尸程序/网络没有检测能力;并且特征串的提取往往依赖于人工分析,难以应对目前急剧增长的僵尸程序数量.虽然文献[48]中进行了自动提取网络流量特征内容的尝试并取得了很好的实验结果,但这种方式是否具有一般性还有待进一步加以研究.

2.4.2 基于网络流量行为特征的检测技术

由于基于内容特征的检测方法具有一定的局限性,而研究者又认为僵尸网络的通信行为具有时间上的关联性和群体相似性,因此期望通过对网络流量进行分析找出更为一般性的网络行为异常模式以进行僵尸网络的检测.

Zamboni 等人根据同一僵尸网络中多个 bot 网络流量的相似性,提出了一种检测方法 TAMD[49].TAMD 从 3 个角度定义主机流量的相似:一是相同目的地址且通信频繁,二是流量内容类似,三是平台相同.TAMD 通过从这 3 个角度对网络流量进行聚合来检测 bot.Nagaraja 等人提出了一种通过网络流量分析对结构化 P2P 僵尸网络进行检测的方法 BotGrep[50],BotGrep 需要对 ISP 骨干网的流量进行采集,得到网络节点之间的流量分布图,

然后通过随机游走(random walk)方法从图中检测出结构化 P2P 网络的子图,再结合其他如蜜罐等检测系统的结果来判断是否为僵尸网络.

理想状态下,基于网络流量行为的检测方法不容易被逃避,且具有检测未知僵尸网络的能力.但目前,多数这类检测方法在精确度和可部署性方面还无法达到实际应用的需要,其主要困难在于:

(1) 僵尸网络的通信行为复杂多样,很难对异常行为准确定义,通过聚类等自动学习的方式很难保证精确度;

(2) 背景流量同样复杂多样,很难对正常和异常进行区分;

(3) 网络流量数据量极大,而通信行为进行分析往往需要借助采用计算量很大的机器学习等算法,难以做到实时检测.

2.4.3 基于关联分析的检测技术

由于 bot 受 botmaster 的控制进行恶意攻击活动,所以其通信行为往往和一些恶意事件,如 DDoS 攻击、扫描、二进制文件下载等在时间上具有关联性.Gu 等人基于这一特性,在前期工作 BotHunter[51]的基础上又提出了 BotSniffer[52]和 BotMiner[53]两种检测方法.BotSniffer 基于对同一局域网中 bot 活动的时间和空间上关联性(spatial-temporal correlation)的假设,从网络中的 IRC 以及 HTTP 流量中识别出可疑的僵尸网络命令与控制通信,然后再结合扫描、二进制文件下载、spam 等异常事件日志进行关联分析来进行检测.BotMiner 尝试实现不依赖于具体协议的检测方法,通过将所有的流量按目的地址和端口进行聚合作为基本单位,再根据一系列的流量属性进行聚类分析以得到通信行为类似的组,再结合异常事件的日志进行关联分析来检测出可疑的 bot 组.除了 Gu 等人的工作以外,最近发表的 RB-Seeker[54]也采用了关联分析的方法.先通过网络流量数据关联 spam 信息以及 DNS 的日志记录找出可疑域名,再对可疑域名进行探测,并通过机器学习的方法来检测出恶意域名,然后再和 DNS 日志记录进行关联来找出可能的 bot.

把网络行为和一些明确的恶意事件与数据进行关联可以缩小检测范围,提高精确度.但目前,这方面的研究仍然有其局限性.BotHunter 和 BotSniffer 需要依赖于内容特征以及特定类型的僵尸网络通信协议,BotMiner 虽然不依赖于特定的协议和僵尸网络拓扑结构,但需要进行计算量很大的聚类分析,难以保证精确度而且实时性不好.RB-Seeker 也使用了难以保证精确度及实时性的机器学习等方法,且其只针对特定的僵尸网络活动.

2.4.4 基于应用数据和日志分析的检测技术

除了网络通信以外,僵尸网络的一些行为特征,如群体相似性等,也会体现在其所使用的一些网络服务,如 DNS、邮件服务的日志记录中,研究者尝试从这类数据中找出具有异常特征的记录来识别出可能的僵尸网络.

Choi 等人在文献[55]中提出 bot 主机对控制服务器的 DNS 查询具有群体活动的特点,他们根据时间段对查询记录按域名进行分组,如果同一个域名在不同时间段内的查询 IP 地址有很高的重合度,则表明这些 IP 地址代表的主机是可疑的 bot,而该域名为可疑的控制服务器.

僵尸网络所发出的垃圾邮件也具有一定的群组相似性.Zhuang 等人对垃圾邮件的内容进行分析,根据内容的相似性来对垃圾邮件进行分组,再对分组中的发送者 IP 地址进行分析来识别出不同的僵尸网络[56].Xie 等人的研究借鉴了这种思想,他们提出一种自动生成垃圾邮件特征码的方法 AutoRE,以识别僵尸网络发出的垃圾邮件[57].AutoRE 通过提取 E-mail 中的 URL 来生成特征码,然后对具有类似 URL 特征码的 E-mail 及其发送者 IP 地址进行分组,再根据 E-mail 分组的 IP 地址分布和持续时间来判断发送者是否为僵尸网络 bot.

为提高垃圾邮件的发送成功率,一些僵尸网络通过 bot 自动注册和激活 hotmail,gmail 等邮件服务商帐号,然后登录到服务器上发送垃圾邮件.Zhao 等人设计并实现了通过对邮件服务器帐号激活日志和登录日志进行分析来检测可疑 bot 以及相关邮件帐号的系统 BotGraph[58].BotGraph 包括两种检测方法:一种方法从帐号激活日志中分析单个 IP 地址突发的帐号激活操作来判断该 IP 是否为可疑的 bot;另一种检测方法的异常定义为邮件帐号的 IP 地址共享行为,可疑的 IP 地址会登录多个邮件帐号,而可疑的邮件帐号会在多个 IP 地址登录.

2.5 僵尸网络的主动遏制技术

在通过应用蜜罐、行为和特征分析以及检测等各种技术获得僵尸网络的相关信息,如 bot 的地址、僵尸程

序感染源以及命令与控制服务器的地址和域名后,需要进一步通过黑名单、恶意域名清除等方式来抑制僵尸网络的传播和攻击以及关停已经确认的僵尸网络.

通过路由和 DNS 黑名单的方式屏蔽恶意的 IP 和域名是一项简单而有效的技术,如 CNCERT/CC 对 Conficker 僵尸网络的命令与控制域名即采用了 sinkhole 技术进行屏蔽.对于终端用户和网络管理员来说,主要问题是如何获得恶意 IP 地址以及域名的数据.目前,已有大量的研究机构和个人在网络上共享了通过僵尸程序分析、IDS 日志分析等方法获得的恶意 IP 地址和域名的黑名单.这一方面的研究工作主要关注于黑名单的及时性和准确性.Sheng 等人对钓鱼网址黑名单的及时性和准确性进行了系统的测量[59],Felegyhazi 等人探讨了通过关联分析的方法基于已有的域名黑名单提前预测恶意域名的可能性[60].

针对基于 Web 的传播和攻击方式的流行,Google 启动了 Google Safe Browsing 项目[28]来收集并发布挂马和僵尸程序宿主网页以及钓鱼网站,并以黑名单的形式集成在 firefox 和 chrome 浏览器中.其他厂商也进行了类似的工作,目前,各主流的 Web 浏览器均加入了黑名单机制来阻止用户对恶意网址的访问.

更为直接的方法是直接关停僵尸网络所使用的域名或关闭其命令与控制服务器的网络连接.这种方式面临的困难主要是管理和政策方面的问题.一个僵尸网络所使用的域名和控制服务器往往分布在不同的行政区域,各区域管理机构难以协同对其进行处置.而且部分地域对恶意网络活动缺乏监管,导致大量的恶意域名和控制服务器集中在所谓的安全区域(bulletin proof domain registrar and ISP),难以得到处置.近年来,一些大型的企业、安全机构和各国管理机构开始尝试对僵尸网络的大规模的协同处置行动.对 Waledac,Rustock 进行的域名关停以及断开存在大量控制服务器的 ISP McColo 的网络连接,都取得了明显的效果.就此也有一些相应的研究工作,Liu 等人结合中国对 cn 域名的监管以及 enom 对恶意域名的打击这两个案例,讨论了域名监管政策对恶意网络活动的影响[61].Stone-Gross 等人通过跟踪僵尸网络控制服务器以及恶意网站的地址建立了对 ISP 进行评分的信誉系统,以促进 ISP 对其域内的恶意站点进行清理[62].

3 讨 论

3.1 目前僵尸网络防御的主要问题

虽然僵尸网络的研究取得了显著的进展,已初步形成整体的防御体系,但目前仍然不能有效地遏制僵尸网络的发展态势,我们认为还存在技术和非技术两个方面的问题.

技术方面主要存在 3 点问题:一是僵尸程序分析和僵尸网络逆向工程的可扩展性问题.目前,以人工为主的僵尸程序和僵尸网络工作机制分析无法应对爆炸性增长的僵尸程序数量;二是缺少新的可实际部署的检测技术,目前所提出的新检测方法仍然达不到实际部署的准确度或性能需要;三是技术上缺少对大范围跨地域信息共享和协作响应的支持,使得各网络管理域及行政区域之间的信息共享和协作无法形成高效以及长效的机制.

非技术方面同样主要存在 3 点问题:一是全球范围内的信息共享的协作响应和联动面临各种非技术,如法律、政策等方面的阻力;二是需要进一步促使 ISP 加强对其域内互联网资源的管理和自律,使其能够及时发现和清理管理域内的恶意域名或地址;三是从法律上需要加强对互联网犯罪惩戒力度,提高对攻击者的心理威慑.

3.2 僵尸网络的发展趋势

一是规模方面,有组织的犯罪集团控制少量超大规模僵尸网络,并在不断发展增强僵尸网络自身安全性的技术手段来与安全社区进行技术博弈与竞争,而大量个人则利用自动化恶意套件建立小型化僵尸网络,通过提高代价来躲避安全监测与响应;二是智能化,传播、命令控制及攻击手段更加精细,更为充分地利用社交网络来进行传播与控制,同时,逐步扩展至移动设备终端等新型计算环境[63];三是僵尸网络背后的地下经济利益驱动更加明显,盈利方式也更加多样化和隐蔽化.

3.3 可能的进一步研究方向

综合以上讨论,我们认为,僵尸网络领域可能的进一步研究方向包括:(1) 新型僵尸网络的发现和工作机制分析;(2) 可扩展的僵尸网络逆向工程方法;(3) 可部署的僵尸网络检测技术;(4) 大范围信息共享和协同响应的

支持技术;(5) 对僵尸网络背后的地下经济市场的研究.

4 总 结

近年来,僵尸网络在多样化传播途径、更为专业化的攻击方式以及具备更强的自身安全性的命令与控制机制等方面,通过与安全社区的技术博弈不断地进化和发展,已经成为互联网多种类型安全威胁的主要源头.业界对僵尸网络的工作机制、行为特征已经有了较为深入的理解,提出了多种僵尸网络检测方法,并在不同范围的网络管理域内开展了有针对性的主动响应,已经形成了由安全威胁监测、工作机制分析、特征分析、在线检测及主动遏制这5个环节所组成的僵尸网络整体防御技术体系.本文对这5个技术环节中近年来主要的研究工作进行了综述与分析,然而,由于网络体系结构的限制与僵尸网络自身复杂性所带来的技术难题以及僵尸网络威胁跨管理域所带来的协调沟通等非技术性困难,如何有效地遏制僵尸网络威胁仍然需要持续而深入的研究.

致谢 感谢清华大学信息网络工程研究中心网络和信息安全技术研究室的各位同学给予本文工作的建议.

References:

[1] Franklin J, Paxson V, Perrig A, Savage S. An inquiry into the nature and causes of the wealth of Internet miscreants. In: Proc. of the 14th ACM Conf. on Computer and Communications Security. Alexandria: ACM Press, 2007. 375–388. [doi: 10.1145/1315245.1315292]

[2] Holz T, Engelberth M, Freiling F. Learning more about the underground economy: A case-study of keyloggers and dropzones. In: Backes M, Ning P, eds. Proc. of the Computer Security—ESORICS 2009. LNCS 5789, Heidelberg, Berlin: Springer-Verlag, 2009. 1–18. [doi: 10.1007/978-3-642-04444-1_1]

[3] Zhuge JW, Holz T, Song CY, Guo JP, Han XH, Zou W. Studying malicious websites and the underground economy on the Chinese Web. In: Proc. of the Managing Information Risk and the Economics of Security. Springer-Verlag, 2009. 225–244. [doi: 10.1007/978-0-387-09762-6_11]

[4] Fossi M, Johnson E, Turner D, Mack T, Blackbird J, McKinney D, Low MK, Adams T, Laucht MP, Gough J. Symantec report on the underground economy: July 2007 to June 2008. Technical Report, Symantec Corporation, 2008. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

[5] Turner D, Fossi M, Johnson E, Mark T, Blackbird J, Entwise S, Low M, McKinney D, Wueest C. Symantec global Internet security threat report: Trends for 2008. White Paper. Symantec Enterprise Security, 2009.

[6] Fossi M, Turner D, Johnson E, Mack T, Adams T, Blackbird J, Entwisle S, Graveland B, McKinney D, Mulcahy J. Symantec global Internet security threat report: Trends for 2009. White Paper. Symantec Enterprise Security, 2010.

[7] Fossi M, Turner D, Johnson E, Mack T, Adams T, Blackbird J, Entwisle S, Graveland B, McKinney D, Mulcahy J. Symantec global Internet security threat report: Trends for 2010. White Paper. Symantec Enterprise Security, 2011.

[8] Leder F, Werner T. Know your enemy: Containing conficker. Technical Report, The Honeynet Project, 2009.

[9] Sinha P, Boukhtouta A, Belarde VH, Debbabi M. Insights from the analysis of the Mariposa botnet. In: Proc. of the 5th Int'l Conf. on Risks and Security of Internet and Systems (CRiSIS 2010). 2010. 1–9. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5764915&isnumber=5764913 [doi: 10.1109/CRISIS.2010.5764915]

[10] Sun YD, Li D. Overview of botnet. Computer Applications, 2006,26(7):1628−1630 (in Chinese with English abstract).

[11] Zhuge JW, Han XH, Ye ZY, Zou W. Discover and track botnets. In: Proc. of the Chinese Symp. on Network and Information Security. Beijing, 2005 (in Chinese with English abstract). http://cpfd.cnki.com.cn/Article/CPFDTOTAL-ZGTH200508006025.htm

[12] Zhou YL, Cui X. Detection and countermeasure against botnet. In: Proc. of the Chinese Symp. on Network and Information Security. Beijing, 2005 (in Chinese with English abstract). http://cpfd.cnki.com.cn/Article/CPFDTOTAL-ZGTH200508006019.htm

[13] Zhuge JW, Han XH, Zhou YL, Ye ZY, Zou W. Research and development of botnets. Journal of Software, 2008,19(3):702−715 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/702.htm [doi: 10.3724/SP.J.1001.2008.00702]

[14] Zhu ZS, Lu GH, Chen Y, Fu ZJ, Roberts P, Keesook H. Botnet research survey. In: Proc. of the COMPSAC 2008. 2008. 967–972. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4591703&isnumber=4591503 [doi: 10.1109/COMPSAC.2008.205]

[15] Bailey M, Cooke E, Jahanian F, Xu Y, Karir M. A survey of botnet technology and defenses. In: Proc. of the 2009 Cybersecurity Applications and Technology Conf. for Homeland Security. IEEE Computer Society, 2009. 299−304. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4804459&isnumber=4804414 [doi: 10.1109/CATCH.2009.40]

[16] Thomas K, Nicol DM. The Koobface botnet and the rise of social malware. In: Proc. of the 5th Int'l Conf. on Malicious and Unwanted Software (MALWARE 2010). 2010. 63−70. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5665793&isnumber=5665785 [doi: 10.1109/MALWARE.2010.5665793]

[17] Binsalleeh H, Ormerod T, Boukhtouta A, Sinha P, Youssef A, Debbabi M, Wang L. On the analysis of the Zeus botnet crimeware toolkit. In: Proc. of the 8th Annual Int'l Conf. on Privacy Security and Trust (PST 2010). 2010. 31−38. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5593240&isnumber=5593224 [doi: 10.1109/PST.2010.5593240]

[18] Stone-Gross B, Cova M, Cavallaro L, Gilbert B, Szydlowski M, Kemmerer R, Kruegel C, Vigna G. Your botnet is my botnet: Analysis of a botnet takeover. In: Proc. of the 16th ACM Conf. on Computer and Communications Security. Chicago: ACM Press, 2009. 635−647. [doi: 10.1145/1653662.1653738]

[19] Cho CY, Caballero J, Grier C, Paxson V, Song D. Insights from the inside: A view of botnet management from infiltration. In: Proc. of the 3rd USENIX Conf. on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More. San Jose: USENIX Association, 2010. http://dl.acm.org/citation.cfm?id=1855686.1855688

[20] Nunnery C, Sinclair G, Kang BB. Tumbling down the rabbit hole: Exploring the idiosyncrasies of botmaster systems in a multi-tier botnet infrastructure. In: Proc. of the 3rd USENIX Conf. on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More. San Jose: USENIX Association, 2010. http://dl.acm.org/citation.cfm?id=1855686.1855687

[21] Sinclair G, Nunnery C, Kang BBH. The waledac protocol: The how and why. In: Proc. of the 4th Int'l Conf. on Malicious and Unwanted Software (MALWARE 2009). 2009. 69−77. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5403015&isnumber=5403012 [doi: 10.1109/MALWARE.2009.5403015]

[22] Stover S, Dittrich D, Hernandez J, Dietrich S. Analysis of the storm and nugache trojans: P2P is here. ; login, 2007,32(6). http://www.usenix.org/publications/login/2007-12/pdfs/stover.pdf

[23] Holz T, Steiner M, Dahl F, Biersack E, Freiling F. Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm. In: Proc. of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats. San Francisco: USENIX Association, 2008. 1−9. http://dl.acm.org/citation.cfm?id=1387709.1387718

[24] Kanich C, Kreibich C, Levchenko K, Enright B, Voelker GM, Paxson V, Savage S. Spamalytics: An empirical analysis of spam marketing conversion. In: Proc. of the 15th ACM Conf. on Computer and Communications Security. Alexandria: ACM Press, 2008. 3−14. [doi: 10.1145/1455770.1455774]

[25] Kreibich C, Kanich C, Levchenko K, Enright B, Voelker GM, Paxson V, Savage S. Spamcraft: An inside look at spam campaign orchestration. In: Proc. of the 2nd USENIX Conf.on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More. Boston: USENIX Association, 2009. 4. http://dl.acm.org/citation.cfm?id=1855676.1855680

[26] Stewart J. Inside the storm: Protocols and encryption of the storm botnet. In: Proc. of the Black Hat Technical Security Conf. 2008. http://www.blackhat.com/presentations/bh-usa-08/Stewart/BH_US_08_Stewart_Protocols_of_the_Storm.pdf

[27] Rajab MA, Zarfoss J, Monrose F, Terzis A. A multifaceted approach to understanding the botnet phenomenon. In: Proc. of the 6th ACM SIGCOMM Conf. on Internet Measurement. Rio de Janeriro: ACM Press, 2006. 41−52. [doi: 10.1145/1177080.1177086]

[28] Provos N, Mavrommatis P, Rajab MA, Monrose F. All your iFRAMEs point to us. In: Proc. of the 17th Conf. on Security Symp. San Jose: USENIX Association, 2008. 1−15. http://dl.acm.org/citation.cfm?id=1496711.1496712

[29] Caballero J, Grier C, Kreibich C, Paxson V. Measuring pay-per-install: The commoditization of malware distribution. In: Proc. of the USENIX Security. 2011. http://dl.acm.org/citation.cfm?id=2028067.2028080

[30] Daswani N, Stoppelman M. The anatomy of Clickbot.A. In: Proc. of the 1st Conf. on First Workshop on Hot Topics in Understanding Botnets. Cambridge: USENIX Association, 2007. 11. http://dl.acm.org/citation.cfm?id=1323128.1323139

[31] Miller B, Pearce P, Grier C, Kreibich C, Paxson V. What's clicking what? Techniques and innovations of today's clickbots. In: Holz T, Bos H, eds. Proc. of the Detection of Intrusions and Malware, and Vulnerability Assessment. LNCS 6739, Heidelberg: Springer Berlin, 2011. 164−183. [doi: 10.1007/978-3-642-22424-9_10]

[32] Dittrich D, Dietrich S. Discovery techniques for P2P botnets. Technical Report, Stevens Institute of Technology CS, 2008. http://www.cs.stevens.edu/~spock/pubs/dd2008tr4.pdf

[33] Kartaltepe E, Morales J, Xu SH, Sandhu R. Social network-based botnet command-and-control: Emerging threats and countermeasures. In: Zhou J, Yung M, eds. Proc. of the Applied Cryptography and Network Security. LNCS 6123, Heidelberg, Berlin: Springer-Verlag, 2010. 511−528. [doi: 10.1007/978-3-642-13708-2_30]

[34] Holz T, Gorecki C, Rieck K, Freiling FC. Measuring and detecting fast-flux service networks. In: Proc. of the 15th Annual Network and Distributed System Security Symp. 2008. https://www.isoc.org/isoc/conferences/ndss/08/papers/16_measuring_and_detecting.pdf

[35] Nazario J, Holz T. As the net churns: Fast-Flux botnet observations. In: Proc. of the 3rd Int'l Conf. on Malicious and Unwanted Software (MALWARE 2008). 2008. 24–31. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4690854&isnumber=4690850 [doi: 10.1109/MALWARE.2008.4690854]

[36] Riden J. Know your Enemy: Fast-Flux service networks. The Honeynet Project, 2008.

[37] Provos N. A virtual honeypot framework. In: Proc. of the 13th Conf. on USENIX Security Symp. Vol.13. San Diego: USENIX Association, 2004. 1. http://dl.acm.org/citation.cfm?id=1251375.1251376

[38] Seifert C, Steenson R, Holz T, Bing Y, Davis MA. Know your Enemy: Malicious Web servers. The Honeynet Project, 2007.

[39] Nazario J. PhoneyC: A virtual client honeypot. In: Proc. of the 2nd USENIX Conf. on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More. Boston: USENIX Association, 2009. 6. http://dl.acm.org/citation.cfm?id=1855676.1855682

[40] Antonatos S, Polakis I, Petsas T, Markatos EP. A systematic characterization of IM threats using honeypots. In: Proc. of the 17th Annual Network and Distributed System Security Symp. 2010. http://www.isoc.org/isoc/conferences/ndss/10/pdf/09.pdf

[41] Stringhini G, Kruegel C, Vigna G. Detecting spammers on social networks. In: Proc. of the 26th Annual Computer Security Applications Conf. Austin: ACM Press, 2010. 1–9. [doi: 10.1145/1920261.1920263]

[42] Cho CY, Babi D, Shin ECR, Song D. Inference and analysis of formal models of botnet command and control protocols. In: Proc. of the 17th ACM Conf. on Computer and Communications Security. Chicago: ACM Press, 2010. 426–439. [doi: 10.1145/1866307.1866355]

[43] Caballero J, Poosankam P, Kreibich C, Song D. Dispatcher: Enabling active botnet infiltration using automatic protocol reverse-engineering. In: Proc. of the 16th ACM Conf. on Computer and Communications Security. Chicago: ACM Press, 2009. 621–634. [doi: 10.1145/1653662.1653737]

[44] Levchenko K, Pitsillidis A, Chachra N, Enright B, Félegyházi M, Grier C, Halvorson T, Kanich C, Kreibich C, Liu H, McCoy D, Weaver N, Paxson V, Voelker GM, Savage S. Click trajectories: End-to-End analysis of the spam value chain. In: Proc. of the IEEE Symp. on Security and Privacy (Oakland 2011). 2011. 431–446. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5958044&isnumber=5958008

[45] Kanich C, Weaver N, McCoy D, Halvorson T, Kreibich C, Levchenko K, Paxson V, Voelker GM, Savage S. Show me the money: characterizing spam-advertised revenue. In: Proc. of the 20th Conf. on USENIX Security Symp. 2011. http://dl.acm.org/citation.cfm?id=2028067.2028082

[46] John JP, Moshchuk A, Gribble SD, Krishnamurthy A. Studying spamming botnets using Botlab. In: Proc. of the 6th USENIX Symp. on Networked Systems Design and Implementation. Boston: USENIX Association, 2009. 291–306. http://dl.acm.org/citation.cfm?id=1558977.1558997

[47] Pitsillidis A, Levchenko K, Kreibich C, Kanich C, Voelker GM, Paxson V, Weaver N, Savage S. Botnet judo: Fighting spam with itself. In: Proc. of the 17th Annual Network and Distributed System Security Symp. 2010. http://www.isoc.org/isoc/conferences/ndss/10/pdf/12.pdf

[48] Rieck K, Schwenk G, Limmer T, Holz T, Laskov P. Botzilla: Detecting the "phoning home" of malicious software. In: Proc. of the 2010 ACM Symp. on Applied Computing. Sierre: ACM Press, 2010. 1978–1984. [doi: 10.1145/1774088.1774506]

[49] Yen TF, Reiter M. Traffic aggregation for malware detection. Assessment. In: Zamboni D, ed. Proc. of the Detection of Intrusions and Malware, and Vulnerability. LNCS 5137, Heidelberg, Berlin: Springer-Verlag, 2008. 207–227. [doi: 10.1007/978-3-540-70542-0_11]

[50] Nagaraja S, Mittal P, Hong CY, Caesar M, Borisov N. BotGrep: Finding P2P bots with structured graph analysis. In: Proc. of the 19th USENIX Conf. on Security. Washington: USENIX Association, 2010. 7. http://dl.acm.org/citation.cfm?id=1929820.1929830

[51] Gu GF, Porras P, Yegneswaran V, Fong M, Lee WK. BotHunter: Detecting malware infection through IDS-driven dialog correlation. In: Proc. of the 16th USENIX Security Symp. on USENIX Security Symp. Boston: USENIX Association, 2007. 1–16. http://dl.acm.org/citation.cfm?id=1362903.1362915

[52] Gu GF, Zhang JJ, Lee WK. BotSniffer: Detecting botnet command and control channels in network traffic. In: Proc. of the 15th Annual Network and Distributed System Security Symp. 2008. https://www.isoc.org/isoc/conferences/ndss/08/papers/17_botsniffer_detecting_botnet.pdf

[53] Gu GF, Perdisci R, Zhang JJ, Lee WK. BotMiner: Clustering analysis of network traffic for protocol- and structure-independent botnet detection. In: Proc. of the 17th Conf. on Security Symp. San Jose: USENIX Association, 2008. 139–154. http://dl.acm.org/citation.cfm?id=1496711.1496721

[54] Hu X, Knysz M, Shin KG. Rb-Seeker: Auto-Detection of redirection botnets. In: Proc. of the 16th Annual Network and Distributed System Security Symp. 2009. http://www.isoc.org/isoc/conferences/ndss/09/pdf/10.pdf

[55] Choi H, Lee H, Lee H, Kim H. Botnet detection by monitoring group activities in DNS traffic. In: Proc. of the 7th IEEE International Conf. on Computer and Information Technology (CIT 2007). 2007. 715−720. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4385169&isnumber=4385041 [doi: 10.1109/CIT.2007.90]

[56] Zhuang L, Dunagan J, Simon DR, Wang HJ, Tygar JD. Characterizing botnets from email spam records. In: Proc. of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats. San Francisco: USENIX Association, 2008. 1−9. http://dl.acm.org/citation.cfm?id=1387709.1387711

[57] Xie YL, Yu F, Achan K, Panigrahy R, Hulten G, Osipkov I. Spamming botnets: Signatures and characteristics. In: Proc. of the ACM SIGCOMM 2008 Conf. on Data communication. Seattle: ACM Press, 2008. 171−182. [doi: 10.1145/1402958.1402979]

[58] Zhao Y, Xie YL, Yu F, Ke QF, Yu Y, Chen Y, Gillum E. BotGraph: Large scale spamming botnet detection. In: Proc. of the 6th USENIX Symp. on Networked Systems Design and Implementation. Boston: USENIX Association, 2009. 321−334. http://dl.acm.org/citation.cfm?id=1558977.1558999

[59] Sheng S, Wardman B, Warner G, Cranor LF, Hong J, Zhang CS. An empirical analysis of phishing blacklists. In: Proc. of the 6th CEAS. 2009. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.165.520

[60] Felegyhazi M, Kreibich C, Paxson V. On the potential of proactive domain blacklisting. In: Proc. of the 3rd USENIX Conf. on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More. San Jose: USENIX Association, 2010. 6. http://dl.acm.org/citation.cfm?id=1855686.1855692

[61] Liu H, Levchenko K, Félegyházi M, Maier G, Voelker GM, Savage S. On the effects of registrar-level intervention. In: Proc. of the 4th USENIX Conf. on Large-Scale Exploits and Emergent Threats. Boston: USENIX Association, 2011. http://dl.acm.org/citation.cfm?id=1972441.1972448

[62] Stone-Gross B, Kruegel C, Almeroth K, Moser A, Kirda E. FIRE: FInding rogue nEtworks. In: Proc. of the 2009 Annual Computer Security Applications Conf. IEEE Computer Society, 2009. 231−240. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5380682&isnumber=5380502 [doi: 10.1109/acsac.2009.29]

[63] Traynor P, Lin M, Ongtang M, Rao V, Jaeger T, McDaniel P, Porta TL. On cellular botnets: measuring the impact of malicious devices on a cellular network core. In: Proc. of the 16th ACM Conf. on Computer and Communications Security. Chicago: ACM Press, 2009. 223−234. [doi: 10.1145/1653662.1653690]

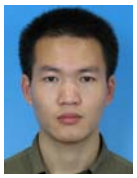
附中文参考文献:

[10] 孙彦东,李东.僵尸网络综述.计算机应用,2006,26(7):1628−1630.

[11] 诸葛建伟,韩心慧,叶志远,邹维.僵尸网络的发现与跟踪.见:中国网络与信息安全技术研讨会论文集.北京,2005.

[12] 周勇林,崔翔.僵尸网络的发现与对策.见:中国网络与信息安全技术研讨会论文集.北京,2005.

[13] 诸葛建伟,韩心慧,周勇林,叶志远,邹维.僵尸网络研究.软件学报,2008,19(3):702−715. http://www.jos.org.cn/1000-9825/19/702.htm [doi: 10.3724/SP.J.1001.2008.00702]



江健(1982－),男,湖北荆门人,博士生,主要研究领域为计算机网络安全.

段海新(1972－),男,博士,研究员,主要研究领域为计算机网络安全.

诸葛建伟(1980－),男,博士,副研究员,CCF 会员,主要研究领域为网络与系统安全.

吴建平(1953－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为计算机网络.