僵尸网络流量检测与控制追踪技术研究

郭晓军,何 磊,赵江波
(西藏民族学院 信息工程学院,陕西 咸阳 712082)

摘 要:借助僵尸网络进行的各种网络攻击对目前互联网的安全已构成严重威胁,对僵尸网络的检测、阻断和控制及僵尸网络控制者跟踪定位已成为当前网络安全研究的热点。文中首先对当前基于网络流量特征识别僵尸网络的方法进行了分类概括,其次对僵尸网络阻断和控制的主要技术进行了归纳整理,最后对当前僵尸网络控制者追踪定位的主要方法进行了梳理总结。现有研究表明,从网络流量角度对僵尸网络进行检测和追踪是非常有效的途经之一,但在准确性和效率方面有待提高。

关键词:网络安全;僵尸网络;流量特征;检测技术;阻断控制;追踪定位
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2013)09-0135-04
doi:10.3969/j.issn.1673-629X.2013.09.034

Research on Botnet Traffic Detection with Control and Tracking

GUO Xiao-jun, HE Lei, ZHAO Jiang-bo
(College of Information Engineering, Tibet Nationalities Institute, Xianyang 712082, China)

Abstract: The various network attack by Botnet has caused serious threats to the current Internet. Botnet detection, blocking and control, and botmaster tracking and positioning have been the hop topics in network security research. Classify current Botnet detection methods based on network traffic features, present primary Botnet blocking and control research and summarize the main technologies on Botmaster traceback. The current related work shows that although detecting and traceback Botnet via network traffic is a effective method, it still need to be improved in accuracy and efficiency facets.

Key words: network security; Botnet; traffic features; detection method; block and control; track and position

0 引 言

僵尸网络(Botnet)是由大量被僵尸程序所感染的主机受到攻击者(称为 Botmaster)所控制而形成的以恶意活动为目的覆盖网络。Botmaster 可以通过控制服务器操控众多被感染的主机发起各种类型的网络攻击行为,如网络钓鱼(Phishing)、发送海量垃圾邮件(Spam)、分布式拒绝服务(DDoS)以及窃取用户隐私信息(Privacy Leak)等等。这些恶意活动不仅给用户带了巨大的经济损失[1],而且使得用户的网络环境面临严峻的安全威胁。

目前,我国早已成为最大的僵尸网络受害国之一,2012 年 3 月份,CNCERT/CC(国家计算机网络应急技术处理协调中心)共发现约 890 万个境内主机被感染了僵尸程序(Bot),较 2010 年相比有较大增加,一些政府网站、知名公司网站及游戏服务器等遭受到多次 DDoS 攻击,给国内的公共互联网环境的安全造成了较大冲击[2]。因此,加强对僵尸网络检测技术的研究是非常必要和关键的,也是有效防御和反制僵尸网络的基础。

针对僵尸网络检测问题,国内外学者已提出了多种方法,如蜜罐检测、特征值检测、DNS 检测、数据挖掘检测等。文中在给出僵尸网络定义和类型的基础上,从网络流量的角度出发,首先针对如何在大流量网络环境中检测是否存在僵尸网络的问题,对当前国内外的研究现状进行了分类归纳;其次,总结了当前最新的僵尸网络阻断和控制技术;最后对 Botmaster 定位及跟踪技术当前研究状况等进行了综述。

1 僵尸网络定义和类型

关于僵尸网络的定义,已有研究文献给出了一些

收稿日期:2012-12-01 **修回日期**:2013-03-04 **网络出版时间**:2013-05-09
基金项目:教育部科学技术研究重点项目(212168);西藏民族学院重点项目(11MYZ04)
作者简介:郭晓军(1983-),男,讲师,研究方向为网络信息安全;何 磊,副教授,研究方向为网络信息安全、无线传感器网络。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130509.1058.031.html

形式化的描述[3-4],为了方便理解,文中仅给出僵尸网络一般意义上的定义。

僵尸网络是指攻击者或控制者通过传播僵尸程序(Bot)感染和控制网络上存在漏洞的若干主机,且与所控制的主机之间建立过命令与控制信道,向其发送若干命令,以达到窃取信息、点击欺诈、DDos 攻击等各种恶意目的。从此定义不难看出,僵尸网络具备四个核心要素:

攻击者或控制者:僵尸网络的所有者;

僵尸终端:通信网络中被攻击者或控制者所控制的计算机、手机等终端设备;

僵尸程序:攻击者或控制者用于控制僵尸终端的恶意程序;

命令控制信道:即 Command and Control Channel(C&C Channel),是攻击者或控制者向僵尸终端发布控制命令所使用的通信方式,包括通信协议、组成结构等,是整个僵尸网络的核心。

僵尸网络结构见图 1。

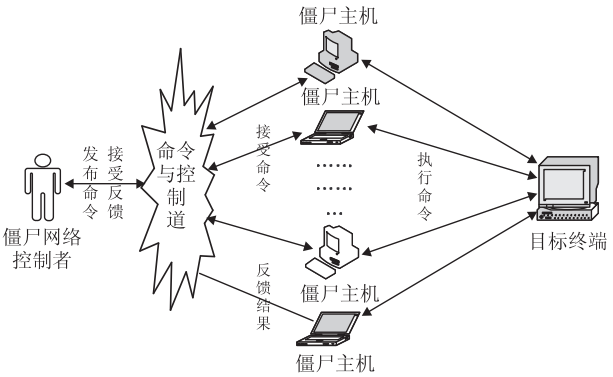

图 1 僵尸网络结构

僵尸网络按不同的标准可以划分为多种类别。由于命令控制信道是整个僵尸网络的核心,因此,文中根据僵尸网络使用的命令与控制的协议对其进行分类[5],如表 1 所示。

表 1 根据 C&C Channel 协议划分的僵尸网络类型

C&C Channel 协议	典型僵尸程序名称
IRC	Agobot, GT-Bot, Rbot, Sdbot
自定义	Mariposa, MegaD,
HTTP	Clickbot, Conficker, Naz, Rustock, Torping, Zeus
P2P	Koobface, Nugache, Phatbot, Sinit, Storm, Waledac

2 僵尸网络检测技术—基于网络流量特征

从网络流量角度来检测僵尸网络的方法主要是利用已知的僵尸网络流量特征(如关键字特征、交互行为特征等)检测当前网络流量中是否存在僵尸网络异常流量。该方法不需要同僵尸控制者进行交互,隐蔽性较好,不会被僵尸网络控制者发现。根据所使用的不同僵尸网络流量特征,可以分为如下几类:

2.1 应用层报文关键字检测法

该方法主要利用僵尸网络交互时产生的数据包应用层内所包含的一些特征字符串来进行识别。由于不同僵尸网络可能会产生不同的特征字符串,因此,该方法还可用来区分不同的僵尸网络类型。例如文献[5]中提到的某些僵尸网络流量会含有“killthread”,“|0d 0a|…|0d 0a|”等特殊指纹。文献[6]分析了基于 IRC 通信协议的 Agobot、sDBot、spyBot 和 GTBot 四种僵尸程序源码,找出了各自的特征字符串以方便检测。

2.2 数据流特征分析检测法

该方法主要利用僵尸网络交互时产生的流量特征来进行识别。由于僵尸网络在运作时会产生与正常通信流量不同的数据流量特征,如通信周期性、Arp 请求速率异常、ICMP 应答速率异常等,因此,当网络中存在僵尸网络通信流量时,可以用该方法来进行检测。

针对基于 IRC 和 HTTP 协议类型的僵尸网络通信,文献[7]利用检测网络中流的某方面特征,如数据包时序、流量持续时间等,来识别基于 IRC(Internet Relay Chat)僵尸网络的 C&C Channel 流量;文献[8]通过一些分类器(如决策树、贝叶斯网络)方法来从网络流量中区分和识别使用 IRC 的僵尸网络流量;文献[9]针对在 ISP(Internet Service Provider)网络层次上检测 IRC 网络流量的问题,给出了一种基于网络数据流统计特征的检测方法,此方法作用在传输层以下,可以很好地保护用户的隐私,并且对加密通信的 IRC 僵尸网络检测也可以进行检测;文献[10]提出了一种通过分析网络流的报文数、报文达到时间间隔等流特征相似性来识别僵尸网络流量的方法,该方法主要适用于检测集中式僵尸网络(如基于 IRC、HTTP 僵尸网络等),该文献也通过实验验证了所提出算法的准确性和有效性。

针对基于 P2P 协议的僵尸网络已成为近年来网络安全领域的研究热点[11-15]。Noh 等人[16]提出了一种基于状态转换的检测方法,此方法通过 7 bit 的状态表示法来描述 P2P 数据流的特征,并借助马尔可夫模型建立多个类型的僵尸网络模式,并以这些模式为基础进行僵尸网络识别。文献[17]在总结 P2P 僵尸网络连接建立速率、数据包 Payload 的大小、upload/download 带宽等流量特征的基础上,应用数据挖掘技术在网络流量中检测 P2P 僵尸网络。针对 P2P 类型僵尸网络从流量角度研究的文献也较多。

此外,也有从 DNS 流量特征的角度来检测僵尸网络的[18]。

2.3 行为特征检测法

僵尸网络行为特征是指僵尸网络在其生命周期过

程中所表现出来一些异常的通信过程和网络流量,如发送垃圾邮件、端口扫描、周期性交互、DNS 查询异常等。利用僵尸网络行为特征检测僵尸网络是该方法的核心思想。在此方法中,典型的代表是文献[19-21]。

文献[19]基于僵尸程序行为的相似性提出了僵尸网络检测系统 Botsniffer,该系统可通过分析僵尸主机与僵尸控制服务器间所产生通信流量的时空关系来达到检测僵尸网络的目的,并在某校园网内进行了测试,测试表明该系统对基于 IRC 协议和 HTTP 协议的僵尸网络具有较好的检测效果。

文献[20]所提出的 BotHunter 检测僵尸网络的方法主要使用了基于开源入侵检测系统 Snort 驱动的会话关联方式。该系统针对僵尸网络存在感染、通信控制、传播、攻击等子环节预先定义相应的模块,并利用这些模块分别对网络流量进行检测,然后再对各模块检测结果进行关联分析和综合评价,从而实现检测僵尸网络的功能。

文献[21]根据僵尸网络内各僵尸主机与僵尸控制服务器通信行为及执行攻击行为具有极大相似性这一基本特性,借助聚类算法分析出网络流记录中存在相似通信模式的主机,并进一步对这些主机在行为记录中的行为进行聚类分析,此方法可以有效检测出多种类型的僵尸网络。

此外还有一些针对特定协议行为特征的僵尸网络识别技术[13,22-23]。

3　僵尸网络阻断和控制技术

僵尸网络的阻断和控制是指在检测出僵尸网络后,通过各种技术手段阻止僵尸网络的蔓延,直至僵尸网络消亡为止。由于相对于僵尸网络检测而言,对僵尸网络的阻断和控制在具体技术上实现较为困难,因此目前关于僵尸网络的阻断和控制方面的研究文献相对较少,主要方法有基于蜜罐主机的渗入和控制[24]、基于 Sybil 攻击[24]以及黑名单[25],路由器“黑洞”技术[26]等。

文献[24]利用特殊的蜜罐主机成功的渗入 Storm 僵尸网络后,利用 Sybil 技术对 P2P 节点的关键词和路由表进行修改,以阻止 Storm 僵尸网络攻击的发生和蔓延。

文献[25] 通过域名黑名单、ISP 级别的跟踪和监测等手段来控制和阻止 FFSN 的蔓延。

文献[26]对于前摄性(即主动攻击性)僵尸网络对抗措施主要包括减少、操控(利用控制命令通道渗透进僵尸网络内部)和漏洞利用(利用僵尸程序 Bug 等)三种策略,可适用于不同拓扑结构和规模的 Botnet,并讨论了这三种措施所带来的法律、道德等问题。

4　僵尸网络控制者追踪定位技术

僵尸网络控制者(Botmaster)追踪和定位主要是指利用一些技术手段找到整个僵尸网络幕后实际的操作或控制主机的确切位置。为逃避检测跟踪,Botmaster 会使用一些跳板主机、代理主机等来保护自己,并且这些跳板主机、代理主机常常会跨越多个不同的网络,这使得对 Botmaster 的跟踪和定位非常困难。因此,当前针对追踪和定位僵尸控制者方面的研究较少,主要有蜜罐方法[27]、蜜罐与数字水印结合的方法[28]及利用云服务环境的方法。

文献[28]首次尝试了利用蜜罐主机向控制服务器响应消息中注入数字水印定位 Botmaster,可对若干 IRC 僵尸网络进行追踪定位,找出僵尸网络控制者。文献[29]给出了一种轻量级的僵尸网络追踪系统,该系统利用本机访问流量自检测、感染僵尸主机黑名单、僵尸程序行为检测等可针对基于 HTTP、IRC、DNS、SMTP 等协议的僵尸网络通信进行识别和跟踪,对 C&C Server 有较好的追踪和定位效果。文献[30]获取僵尸主机与 C&C Server 的通信流量、僵尸主机的内存等,并上传至处于云服务环境中的 Traceserver,然后 Traceserver 利用一些算法解析僵尸主机与 C&C 通信所使用的密钥,并利用该密钥将 Pebbletrace 加入僵尸网络,取代僵尸与 Botmaster 进行通信成功后,Botmaster 程序会获取 Botmaster 主机 IP、OS 等相关信息,并将这些信息返回给 Traceserver。

此外,还有研究者建议管理员将各自管辖网络内已发现的 C&C Server、僵尸主机等联合起来组成社区,并在社区内部共享 C&C Server、僵尸主机与 Botmaster 通信模式信息,以追踪和定位 Botmaster[31]。

5　结束语

僵尸网络以其复杂、灵活和高效的特点已成为当前最具威胁性的网络攻击手段,对整个公共网络环境的安全造成了巨大危害。近年来,关于僵尸网络的检测、阻断控制及 Botmaster 的跟踪已成为网络安全领域的研究热点。文中在介绍了僵尸网络定义及其分类的基础上,重点分析和总结了基于网络流量特征方面检测僵尸网络的方法,并整理了目前在僵尸网络阻断和控制、Botmaster 跟踪定位方面的研究进展。文中综述结果表明,如何提高僵尸网络流量特征的通用性和准确性,提高算法识别率,有效阻断和控制僵尸网络,快速准确定位 Botmaster 等都是进一步值得研究的问题。

参考文献:

[1] McAfee Labs. 迈克菲威胁报告:2010 年第三季度[R]. 美国加利福尼亚州圣克拉拉市:迈克菲公司,2010.

[2] 国家互联网应急中心. 2011 年互联网网络安全态势综述[R]. 北京:国家互联网应急中心,2012.
[3] 王天佐,王怀民,刘 波,等. 僵尸网络中的关键问题[J]. 计算机学报,2012,35(6):1192-1208.
[4] 方滨兴,崔 翔,王 威. 僵尸网络综述[J]. 计算机研究与发展,2011,48(8):1315-1331.
[5] 王新良. 僵尸网络异常流量分析与检测[D]. 北京:北京邮电大学,2011.
[6] Paul B, Vinod Y. An Inside Look at Botnets[M]//Malware Detection. Berlin:Springer-Verlag,2007:171-191.
[7] Strayer W T, Walsh R, Livadas C, et al. Detecting botnets with tight command and control[C]//Proc. of 31st IEEE Conference on Local Computer Networks. USA: IEEE, 2006: 195-202.
[8] Livadas C, Walsh R, Lapsley D, et al. Using machine learning techniques to identify botnet traffic[C]//Proc. of 2nd IEEE LCN Workshop on Network Security. USA: IEEE, 2006: 967-974.
[9] Karasaridis A, Rexroad B, Hoefiin D. Wide-scale botnet detection and characterization[C]//Proc. of USENIX HotBots'07. Berkeley: USENIX Association, 2007: 7-7.
[10] Wang Tao, Yu Shuzheng. Centralized Botnet Detection by Traffic Aggregation[C]//Proc. of 2009 IEEE International Symposium on Parallel and Distributed Processing with Applications. Washington, DC: IEEE CPS, 2009: 86-93.
[11] Wang Binbin, Li Zhitang, Tu Hao, et al. Measuring Peer-to-Peer Botnets Using Control Flow Stability[C]//Proc. of 2009 International Conference on Availability, Reliability and Security. Washington, DC: IEEE CPS, 2009: 663-669.
[12] 于晓聪,董晓梅,于 戈,等. 僵尸网络在线检测技术研究[J]. 武汉大学学报(信息科学版),2010,35(5):578-581.
[13] 于 戈,于晓聪,董晓梅,等. P2P 僵尸网络的快速检测技术[J]. 东北大学学报(自然科学版),2010,31(12):1709-1712.
[14] Yu Xiaocong, Dong Xiaomei, Yu Ge, et al. Online botnet detection by continuous similarity monitoring[C]//Proc. of 2009 International Symposium on Information Engineering and Electronic Commerce. Washington, DC: IEEE CPS, 2009: 145-149.
[15] 刘 丹,李毅超,胡 跃. 多阶段过滤的 P2P 僵尸网络检测方法[J]. 计算机应用,2010,30(12):3354-3356.
[16] Noh Sang-Kyn, Oh Joo-Hyung, Lee Jae-Seo, et al. Detecting P2P botnets using a multi-Phased flow model[C]//Proceedings of the 2009 Third International Conference on Digital Society. Washington, DC: IEEE CPS, 2009: 247-253.
[17] Thuraisingham B. Data mining for security applications: mining concept-drifting data streams to detect Peer-to-Peer botnet traffic[C]//Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI'08). Berlin: Springer-Verlag, 2008.
[18] Choi H, Lee H, Lee H. Botnet detection by monitoring group activities in DNS traffic[C]//Proc. of the 7th IEEE International Conference on Computer and Information Technology. Washington, DC: IEEE CPS, 2007: 715-720.
[19] Gu G, Zhang J, Lee W. Botsniffer: Detecting botnet command and control channels in network traffic[C]//Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08). Berkeley: USENIX Association, 2008.
[20] Gu G, Porra S P, Yegne V, et al. BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation[C]//Proc. of 16th USENIX Security Symposium (Security'07). Berkeley: USENIX Association, 2007.
[21] Gu G, Perdisei R, Zhang J, et al. BotMiner: Clustering Analysis of Network Traffic for Protocol and Structure Independent Botnet Detection[C]//Proceedings of the USENIX Security Symposium (Security'08). Berkeley: USENIX Association, 2008.
[22] 王斌斌. 僵尸网络检测方法研究[D]. 武汉:华中科技大学,2010.
[23] Liu L. Bottracer: Execution-Based Bot-Like Malware Detection[M]//Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2008: 97-113.
[24] Holz T, Steiner M, Dahl F, et al. Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on StormWorm[C]//Proceedings of the First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET'08). Berkeley: USENIX Association, 2008.
[25] Holz T. Measuring and detecting fast-flux service networks[C]//Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08). Berkeley: USENIX Association, 2008.
[26] Leder F, Werner T, Martini P. Proactive botnet countermeasures - an offensive approach[R]. Bonn: University of Bonn, 2009.
[27] Thomas V, Jyoti N. Bot Countermeasures[J]. Journal in Computer Virology, 2007, 3(2): 103-111.
[28] Ramsbrock D, Wang X, Jiang X. A First Step Towards Live Botmaster Traceback[C]//Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection. Berlin: Springer-Verlag, 2008: 59-77.
[29] Takemori K. Host-based traceback; tracking bot and C&C server[C]//Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication. New York, USA: [s. n.], 2009: 400-405.
[30] Lin Wenjie, Lee D. Traceback Attacks in Cloud - Pebbletrace Botnet[C]//Proceedings of the 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW'12). Washington, DC: IEEE CPS, 2012: 417-426.
[31] Mizoguchi S, Takemori K, Miyake Y, et al. Traceback Framework against Botmaster by Sharing Network Communication Pattern Information[C]//Proceedings of the 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'11). Washington, DC: IEEE CPS, 2011: 639-644.

僵尸网络流量检测与控制追踪技术研究

作者： 郭晓军， 何磊， 赵江波， GUO Xiao-jun， HE Lei， ZHAO Jiang-bo
作者单位： 西藏民族学院 信息工程学院,陕西 咸阳,712082
刊名： 计算机技术与发展
ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2013(9)