·热点与综述·　　文章编号：1000-3428(2022)08-0012-13　　文献标志码：A　　中图分类号：TP309

社交僵尸网络发展综述

葛　昕[1]，邹福泰[2]，郭万达[2]，谭　越[2]，李林森[2]

（1.上海理工大学 信息化办公室，上海 200093；2.上海交通大学 电子信息与电气工程学院，上海 200240）

摘　要：随着社交平台的发展，社交媒体网络逐渐成为攻击者进行僵尸网络渗透的理想平台。社交僵尸网络利用社交平台自动化程度高、灵活性强与普及度高等特性构建隐蔽信道进行通信，以达到窃取社交平台用户信息、散布不良信息污染网络环境、引导控制舆论等目的。传统的僵尸网络检测机制无法有效地检测社交僵尸网络，为社交媒体的安全性带来极大的挑战。从社交僵尸网络的概念入手，阐述社交僵尸网络在不同社交平台上的发展脉络和发展趋势，研究不同社交媒体上的社交僵尸网络攻击原理和群体特征以及隐蔽型社交僵尸网络的隐蔽手段。在此基础上，将社交僵尸网络的检测方法分为服务器端检测方法和客户端检测方法，并对近年来出现的基于隐写技术和基于机器学习的检测方法进行分析，同时给出社交僵尸网络的反制技术和接管方法的研究现状及发展思路，并对该领域的未来研究方向进行展望。

关键词：网络安全；社交僵尸网络；命令与控制信道；隐写技术；机器学习

开放科学（资源服务）标志码（OSID）：

中文引用格式：葛昕，邹福泰，郭万达，等.社交僵尸网络发展综述[J].计算机工程，2022，48(8)：12-24.

英文引用格式：GE X，ZOU F T，GUO W D，et al.Review on development of social botnets[J].Computer Engineering，2022，48(8)：12-24.

Review on Development of Social Botnets

GE Xin[1]，ZOU Futai[2]，GUO Wanda[2]，TAN Yue[2]，LI Linsen[2]

（1.Information Office，University of Shanghai for Science and Technology，Shanghai 200093，China；
2.School of Electronic Information and Electrical Engineering，Shanghai JiaoTong University，Shanghai 200240，China）

【Abstract】With the development of social platforms，social media networks have gradually become an ideal platforms for attackers to infiltrate Botnets.Social botnets utilize the high flexibility，degree of automation，and popularity of social platforms to create covert channels for communication to steal social media platform user information，disseminate bad information to pollute the network environment，and control public opinion.Traditional botnet detection mechanisms cannot effectively detect social botnets，causing significant challenges to social media security.From the concept of social botnets，the developmental context and trends of social botnets on different social platforms are explained.In addition，the attack principles and group characteristics of social botnets on different social media and the concealment methods of covert social botnets are analyzed.On this basis，the detection methods of social botnets are divided into server-side and client-side，and the detection methods based on steganography and machine learning in recent years are analyzed.Furthermore，the research status and development ideas of the countermeasure technology and takeover method of social botnets are discussed，and future research directions in this field are suggested.

【Key words】cyber security；social Botnets；Command and Control（C&C）channels；steganography；machine learning

DOI：10.19678/j.issn.1000-3428.0061381

0　概述

社交网络为人们提供了模拟现实生活的社交平台，已成为现代社会建立社会关系的重要方式。近年来，世界各国主要的网络社交平台用户数量不断提升，以我国的新浪微博平台为例，截至2017年9月，微博单月内活跃用户数量接近4亿，单日内的活跃用户近2亿。微博具有用户数量大、消息传播速度快等特点，已成为人们讨论新闻、分享观点的重要平台之一。文献[1]研究了即时信息对微博热点新闻进行情感分类的方法，

基金项目：国家重点研发计划（2018YFB0803503）。

作者简介：葛　昕（1976—），男，工程师、硕士，主研方向为网络安全；邹福泰（通信作者），高级工程师、博士；郭万达、谭　越，硕士研究生；李林森，副教授、博士。

收稿日期：2021-04-15　　**修回日期：**2021-11-03　　**E-mail：**zoufutai@sjtu.edu.cn

分析不同人对于相同事件的态度。这类研究针对的是现有社交平台的热点问题，具备很高的社会价值。

随着社交网络的流行与大量用户的涌入，社交网络集中储存了大量的用户个人信息，这些信息包含用户的邮箱、电话号码、兴趣爱好、家庭住址等用户的隐私信息。此外，攻击者发现社交网络中的部分用户安全意识匮乏，且基于用户信任即可建立好友关系和互相访问对方的信息。近年来，社交网络的这些特性开始被攻击者利用，社交僵尸网络应运而生。攻击者通过社交僵尸账号添加用户好友，收集用户信息，给用户的账户安全造成危害。社交网络迅猛发展的势头助长了社交僵尸网络的扩散，使其成为互联网的一种新的威胁。社交僵尸网络具有如下的特征：隐蔽性强，社交网络用户数量大，用户数据较为分散，在海量的正常流量中，僵尸网络产生的流量可以轻松地隐藏自身；传播难度低，人们在社交网络平台上倾向于根据较为主观的个人偏好对用户进行分组，这使得社交僵尸网络能够更加方便地扩大传播范围和窃取隐私数据，同时可以利用其在网络中全新的定位传播错误信息，试图引导公众舆论；危害性大，社交网络平台自身的开放性使得社交僵尸网络可以在平台上发布和部署具有欺骗性的内容和链接，诱使用户对其进行操作，从而向用户植入恶意代码，最终实现对用户主机的控制，达到其恶意目的；持久性，因为社交网络平台的生命周期很长，其中隐藏的社交僵尸网络又很难被检测到，所以社交僵尸网络可以在社交平台上长期地存在且不被发现。

在社交僵尸网络的发展过程中，越来越多的网络安全技术开始被运用。早期的社交僵尸网络普遍使用明文进行传播，较易检测；随后出现了多种多样复杂的、更为隐蔽的社交僵尸网络，如基于图像隐写技术的Stegobot社交僵尸网络[2]、基于网页标签属性域隐蔽的DR-SNbot[3]、基于推文长度的隐写技术的Twitter社交僵尸网络[4]等。由于运用了最新的技术实现了很高的隐蔽性，这些僵尸网络的检测难度往往都很大，危害性相比传统僵尸网络也更大。

综上所述，社交僵尸网络对社交平台有极大的破坏性，同时也危害着用户的个人信息安全与系统安全。因此，研究社交僵尸网络的通信方式、攻击原理和技术，以及相应的防护、接管与反制方案十分重要，具有很高的经济社会价值。

本文从社交僵尸网络安全威胁的根源着手，研究社交僵尸网络的通信原理和运转方式及表现出的群体特征与隐蔽手段，为社交网络的安全防护，尤其是针对运用新技术的社交僵尸网络的检测与防护，提供相关的理论和技术支持。介绍僵尸网络的概念、发展现状与趋势以及社交僵尸网络的概念与发展现状，并分析现有社交僵尸网络的工作机制，对新型的社交僵尸网络——隐蔽型僵尸网络的两类检测方法以及基于机器学习的社交僵尸网络检测方法进行分析，给出社交僵尸网络反制与接管的发展思路。在此基础上，对比分析不同社交僵尸网络检测方法的优缺点，并对未来社交僵尸网络领域的研究方向进行展望。

1　僵尸网络

1.1　僵尸网络概念

僵尸网络（Botnet）是由命令控制信道技术搭建的具有恶意目的的网络[5]。攻击者往往利用僵尸网络来传播僵尸程序，达到控制大量受害者主机的目的。其中，“攻击者”是指能够控制僵尸主机的控制器（Botmaster）。攻击者可以通过一对多的方式高效地控制大量的受害主机发起DDoS攻击、发送垃圾邮件、传播恶意代码、进行点击欺诈以及窃取受控主机敏感信息等。

命令与控制（Command and Control，C&C）信道是僵尸网络的主要特征之一。唯有依赖于C&C信道，攻击者才能达到实时驱动批量僵尸主机执行网络攻击的目的，而控制者能够实现对僵尸主机状态信息及其他数据的回收与攻击策略的实时调整[6]。根据C&C信道的特征不同，传统的僵尸网络被分为基于IRC协议的僵尸网络、基于HTTP协议的僵尸网络、基于P2P结构的僵尸网络、基于Fast-flux[7]技术的僵尸网络、基于Domain Flux[8]技术的僵尸网络、基于URL Flux[9]技术的僵尸网络等。

随着时间的推移，近年来出现了与热门技术紧密相关的僵尸网络，例如在物联网（Internet of Things，IoT）中控制大量设备的IoT僵尸网络、基于区块链技术通信的僵尸网络等。

2016年，基于IoT的Mirai僵尸网络控制了接近50万台物联网设备，实现了高达1.2 Tb/s的网络流量的DDoS攻击[10]。此后，物联网中的DDoS攻击开始成为研究人员的关注对象[11]。近十年来，研究人员或是在Mirai僵尸网络的基础上进行改进，或是设计出更加难以实施防护的IoT僵尸网络。例如文献[12]介绍了Linux Wifatch僵尸网络。这种IoT僵尸网络主要针对感染采用默认用户名密码登录或使用弱密码的IoT设备设计，在感染后Wifatch使用P2P网络，删除主机上的其他恶意软件，关闭该主机的Telnet连接，并在设备日志中记录Telnet关闭的信息。另一种新型的僵尸网络是Linux/IRCTelent，它针对支持IPv6的物联网设备设计，结合了Telnet暴力破解、代码注入、用户名/密码表等多种技术，实现对目标主机的感染和基于IPv4、IPv6协议的泛洪攻击。

区块链技术的发展导致了数字加密货币的流行，比特币则是数字加密货币的代表。区块链具有去中心化、不可篡改性、匿名性等特性，这些特性不仅使其可以作为网络安全防护方案的核心技术，也引起了黑客的注意。黑客开始将比特币引入僵尸网络的C&C通信，借助其特性使得现有的僵尸网络检测方法失效，大幅提升了僵尸网络的隐蔽性。文献[13]介绍一种基于比特币的ZombieCoin僵尸网络，这种僵尸网络采用比

特币的数字签名来隐藏C&C控制信息,从而增加了其检测难度。文献[14]介绍的比特币僵尸网络Testnet,并提出一种实现僵尸网络控制器与僵尸主机之间双向加密通信的僵尸网络。

1.2 僵尸网络发展趋势

随着新技术的不断出现,僵尸网络的传播能力与隐蔽性在逐渐增强,同时网络攻击者开始在不同的平台上部署僵尸网络(如前文所述的出现在物联网上的IoT僵尸网络以及出现在社交平台上的社交僵尸网络)。由此可见,僵尸网络带来的网络安全威胁在不断增加。对于这类安全威胁的防范,潜在的研究不仅在于对僵尸网络的检测,还包括如何对僵尸网络进行反制,降低其传播速度与危害性。

2 社交僵尸网络

基于社交网络的僵尸网络与传统的僵尸网络有着较大的区别:在传统的僵尸网络中,被控制的节点不是控制者拥有的主机,而是存在于网络上的其他用户的主机。而在社交僵尸网络中,被控制的节点是攻击者自行创建的社交账号,攻击者利用僵尸程序控制这些账号执行一些极其类似真实用户的行为来模拟真实账号,该过程如图1所示。

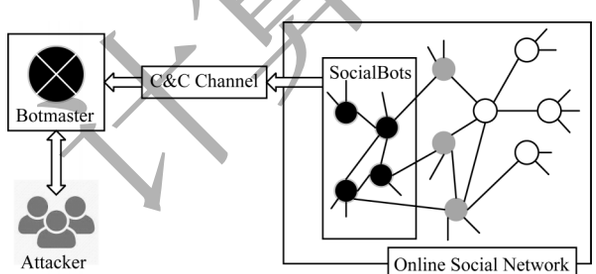

图1 社交僵尸网络概念示意图

Fig.1 Schematic diagram of social botnet concepts

上述差别导致了社交僵尸网络一般不存在感染其他主机的恶意代码,而是通过伪造的URL来诱导人们点击下载恶意代码;社交僵尸网络也不存在特殊的通信协议,因为社交僵尸网络中的通信几乎都是僵尸程序与社交网络服务器之间的基于HTTP的通信。上述不同导致了两者的检测方法的差异性。

2.1 社交僵尸网络定义

定义1(社交僵尸) 社交僵尸是一种特殊的聊天机器人,用于社交网络自动生成消息或者支持某些想法、活动和公共关系,收集追随者信息的虚假账户[15]。

定义2(社交僵尸网络) 社交僵尸网络是指在社交网络中,攻击者出于恶意目的,通过一对多控制结构操纵大量的可模拟真实用户的僵尸账号形成的受控网络[16]。

僵尸账号是攻击者通过人工方法或者运用僵尸程序创建的被社交网络控制的账号,僵尸账号之间不会进行通信。僵尸账号并不只是收集用户信息,还有许多僵尸账号利用与真实用户之间的信任关系传播垃圾信息,严重影响社交网络安全。

2.2 社交僵尸网络恶意行为

社交僵尸网络的恶意行为与普通僵尸网络恶意行为类似,文献[17]将社交僵尸网络的恶意行为分为三大类:消息散布(Information Dispersion),信息收集(Information Gathering)和信息处理(Information Processing),如图2所示。

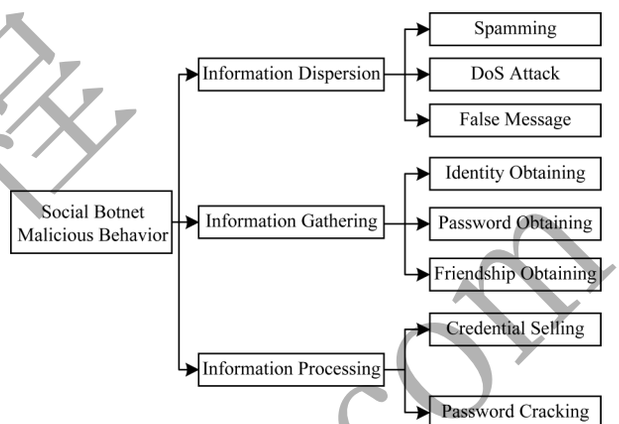

图2 社交僵尸网络恶意行为的分类

Fig.2 Classification of social Botnet malicious behavior

社交僵尸网络恶意行为一般有以下5种形式:

1)污染网络环境。一些僵尸账号隐藏在真实账号之下,通过投放广告赚取点击量,如传播色情、反动信息。一些社交僵尸账号与合法用户之间确立了信任关系,以更加难以发现的方式发布垃圾信息。

2)引导舆论。当一些重大事件发生时,社交僵尸网络通过控制大量社交僵尸账号集体发声制造巨大的网络声浪,引导和控制社会舆论,甚至影响事态的发展,这即所谓的社交网络水军。

3)窃取信息。社交僵尸账号通过与真实的用户建立相互的信任关系,通过与真实用户进行互动,收集真实用户的隐私信息。获取这些信息后,攻击者就可以将它们转卖给营销公司,造成用户信息泄露,导致用户收到大量垃圾短信、垃圾邮件、骚扰电话等。

4)恶意植入。通过与真实用户建立的信任关系发布伪造的URL链接。攻击者可以使用伪造的URL链接进行网络钓鱼、传播病毒、诱导用户下载恶意代码等行为。一些缺乏网络安全意识的用户常会无条件地信任并点击“朋友”发布的链接,从而遭受恶意攻击,甚至被盗取账号、植入主机病毒等。

5)虚假信息传播。由于社交网络的巨大体量和社交僵尸网络强大的消息扩散能力,攻击者可以利用社交网络上的僵尸账号进行谣言的传播。

在国际上已经有社交僵尸网络的恶意行为这一应用的先例:一份针对2010年美国中期大选的文献指出了社交僵尸网络的滥用影响了大选的最终结果[18];2014年,印度的大选中也被发现有运用社交僵尸账号散布对敌对政党不利的新闻的现象[19]。另

外，文献[20]指出，一些国家的政府利用社交僵尸网络来诱导大众发表有利于政府的观点。从国家的层面来讲，现代的战争形成了认知域这一全新的作战维度，与传统战争中的物理域和信息域共同构成了现代战争的三大战场。目前，社交僵尸网络的出现吸引了一些组织的注意力，他们开始尝试将社交僵尸网络运用在向敌人散布虚假的消息或者错误的消息上，这会给敌人的心理造成一些影响，从而左右战争的局势。因此，虽然还没有证据表明社交僵尸网络已经被运用在现代战争中，但是要注意到社交僵尸网络的力量及其对战争胜负的影响力。

综上可见，社交僵尸网络带来的安全威胁是不可小觑的。因此，有必要了解并研究社交僵尸网络的攻击原理与防御方法。

3　社交僵尸网络发展阶段

从第一个知名的社交僵尸网络Koobface[21]出现至今，其攻击形态和攻击技术都发生了巨大的变化，从最初借助社交平台对C&C信道进行弱加密，到运用隐写技术将控制命令隐藏在图片或文本中进行传播的社交僵尸网络，社交僵尸网络的隐蔽性越来越强，种类也变得更加繁杂。

3.1　传统社交僵尸网络阶段

随着社交网络平台的发展，僵尸网络被引入社交网络中。随着2010年第一个成功传播的社交僵尸网络Koobface的出现，一批以传统僵尸网络技术为基础的社交僵尸网络大量产生。下面按照社交僵尸网络所针对的社交平台的不同，分别介绍社交僵尸网络的发展演化历程。

3.1.1　Facebook上的社交僵尸网络

文献[21]介绍了利用社交网络平台进行传播且获得成功的僵尸网络Koobface，其攻击目标是拥有诸如Facebook、MySpace等社交网站账号的个人用户，目标系统为Windows系列操作系统。攻击者通过Koobface可以实现广告推送、恶意软件付费安装、用户信息窃取，进而牟取暴利。Koobface通过社会工程学的方式进行传播。具体来讲，Koobface利用社交网络平台发布恶意视频链接，诱骗用户点击并安装恶意插件从而感染成为僵尸主机。攻击者会事先注册若干blogspot1/bit.ly账号，同时准备好一批被劫持和篡改的网站页面。准备完毕后，Koobface会利用已感染用户的社交账号进行恶意链接的发布和推送（第1个阶段），该链接指向攻击者准备的恶意blogspot/bit.ly链接（第2个阶段），当用户点击访问社交账号上发布的链接时首先会跳转到blogspot/bit.ly中的恶意链接，接着blogspot/bit.ly的链接将会把请求重定向到被劫持和篡改的网页（第3个阶段），通过页面的JavaScript脚本再一次将用户的请求重定向到最终目的地——恶意视频页面（第4个阶段）。还有一些研究人员研究了Koobface僵尸网络的传播及命令控制机制，并分析了Koobface的URL混淆技术，他们认为Koobface仅对C&C信道进行了弱加密。

文献[22]介绍了基于Facebook的社交僵尸网络Yazanbot。该社交僵尸程序可以产生分别针对社交网络信息传递过程和社交关系管理结构的两种操作。前者可以对Facebook上的内容进行读、写等操作；后者则可以产生新的社交关系图。僵尸网络控制者账户可以通过发布不同的命令，实现与社交僵尸账户之间的建立与断开连接操作。同时，僵尸网络控制者账户还能够操纵社交僵尸账户的行为，执行包括命令僵尸账户连接正常的社交账户和仓库内的其他账户、寻找邻居账户、返回收集到的用户信息在内的操作。Facebook提供的API接口和HTTP请求的模板库是Yazanbot工作的主要基础。

其他以Facebook为平台的社交僵尸网络还有文献[23]介绍的Fbbot。Fbbot在随机时间登录Facebook网站首页，获取最新状态，解析后得到相关的命令并进行对应的操作，最终提供反馈信息。Facebook上的社交僵尸网络多利用Facebook提供的Facebook Graph API[24]来进行大规模的社交关系操作，利用社交僵尸程序收集用户的个人信息。

3.1.2　Twitter上的社交僵尸网络

与Koobface同期出现的社交僵尸网络还有文献[25]介绍的基于Twitter的僵尸网络Nazbot。Nazbot使用Twitter上的账户名为upd4t3的僵尸主机接收命令。Nazbot首先向upd4t3的RSS发出HTTP GET请求，Twitter随后返回一个以Base64编码的文本RSS提交给Nazbot。然后Nazbot对该文本进行解码，并从bit.ly网址获取真实的URL，该bit.ly URL重定向到一个独立服务器上的恶意文件。随后Nazbot下载这个恶意文件并将其作为有效载荷解压并执行。最后有效载荷窃取用户的管理信息，并将收集到的信息返回给botmaster控制的服务器。

文献[26]介绍了以明文发布命令的基于Twitter的移动僵尸网络。ZeroFOX威胁研究小组对一个名为Siren的大型僵尸网络进行了调查研究[27]，该网络利用算法生成的Twitter账户所形成的庞大信息网络来发布有效的URL，该URL可以重定向到很多包含色情内容的网站上。随后被控制的僵尸账户通过直接转发受害者的推文，来诱使受害者掉入陷阱。

2013年出现了另一种Twitter上的社交僵尸网络Twitterbot[28]。研究人员使用Twitter作为僵尸网络的C&C信道，直接在Twitter账户上发布僵尸网络命令。僵尸程序通过Twitter网站上的Twitter消息搜索引擎来获取命令，并使用OAuth认证机制和twitter4j API接口开发的应用程序进行通信。Twitterbot使用关键词减少了Twitter消息的可疑度，提高了僵尸网络节点的存活率。

3.1.3 Weibo上的社交僵尸网络

相比于国外的社交僵尸网络，我国出现社交僵尸网络的时间相对较晚。2017年，文献[23]介绍了基于微博平台的社交僵尸网络Wbbot，它通过模拟IE浏览器的行为来访问微博网站，最终获取用户在微博上的个人信息。Wbbot首先尝试从微博主页获取botmaster的状态。随后僵尸程序检查控制命令是否被包含在微博的状态信息中，以及相关命令是否已经被执行。最后僵尸程序会对新的命令进行处理和分析，并执行相应的操作。该社交僵尸网络共存在10个不同的控制命令：6个主机上的行动命令用来获取本地网络信息、Windows系统版本、执行DoS命令、迫使IE浏览器打开一个URL、强迫受害者主机重新绑定域名和IP等；另外4个在线社交网络活动的命令可以控制感染微博账户发布文本消息、更新状态信息、对微博消息进行评论、关注指定账户。

其他Weibo上的社交僵尸网络有文献[3]介绍的DR-SNbot，这种僵尸网络基于新浪博客搭建C&C信道，同时将控制命令隐藏在博文中，并将其发送到多个博客上。文献[29]介绍的基于P2P的社交僵尸网络，通过匿名网络注册账户将加密后的命令释放到账户中。超级节点根据P2P通信机制，使用相同的微博昵称生成算法，并主动通过HTTP请求从微博账户中获取加密命令，增加了防御者跟踪整个僵尸网络的难度，弥补了P2P僵尸网络模型中缺少命令服务器的问题。表1总结了现有的社交僵尸网络的主要特点。由于微博平台的API接口控制较为严格，相比于Twitter和Facebook开放程度较低，因此很少有基于微博的社交僵尸网络研究，而且现有的基于微博的社交僵尸网络的存活时间也相对较短。

表1 不同平台上的社交僵尸网络

Table 1 Social Botnets on different platforms

僵尸名称	社交平台	主机活动	社交行为
Koobface	Facebook MySpace	Steal data	Post message Get message
Yazanbot	Facebook	—	Post status Get status
Fbbot	Facebook	getNetinfo exeCmd, Redirect URL	Post message Get message Add friend
Nazbot	Twitter	Download exe	Get status
Twitterbot	Twitter	Visit URL Download DDOS	Get status Get twitter ID/name
Siren	Twitter	Visit URL Download	Post message Get message Add friend
Wbbot	Weibo	getNetinfo exeCmd Redirect URL	Post status Get status Addfollowing

3.2 新型社交僵尸网络阶段

僵尸网络的C&C信道负责传输僵尸网络的内部控制消息，为防止第三方冒充Botmaster发布命令或窃听C&C通信内容，攻击者通常会在通信过程中引入相关的加密技术。然而，由于发布在社交网络上的社交僵尸网络命令一般是对用户公开的明文，因此社交僵尸网络的C&C信道还必须具备较高的隐蔽性，以防止这些恶意消息被发现，最终导致僵尸网络被检测到并被破坏。为了逃避系统检测，社交僵尸网络开始探索基于信息隐藏技术的隐蔽通道的使用。隐蔽型社交僵尸网络面临如下几个主要问题：如何隐蔽地利用人类的社交习惯，通信的信息如何隐藏，如何更好地逃避检测。因此，隐写技术逐渐被引入到社交僵尸网络的设计与开发过程中。

隐写技术是一门关于信息隐藏的技术和科学，即除预计的信息接收者外，没有人会知道信息的传输（不仅仅是消息的内容）。其中，最常用的隐写技术是基于图像的隐写技术。最具有代表性的隐写技术是JPEG隐写技术Jsteg[30]，其主要思想是在离散余弦变换系数最小的位中隐藏数据，从而保证无法用肉眼看出隐写后与隐写前图像之间的区别。其他的图像隐写技术还有YASS[31]、基于模型的MB[32]、Outguess[33]、F5[34]等。其中YASS随机选取8×8的字块，将隐写信息嵌入到该字块的DCT系数中。

3.2.1 基于图像隐写技术的社交僵尸网络

文献[2]介绍了基于图像隐写技术的Stegobot社交僵尸网络。Stegobot使用社交网络用户共享的图像作为构建C&C通信的通道媒体，采用YASS图像隐写技术在社交网络中建立一个通信的通道，并将其作为社交僵尸网络的C&C信道。Stegobot的设计目的是通过社交网络，比如电子邮件通信网络或允许朋友交换电子邮件的在线社交网络来感染用户。Stegobot感染大量主机，并从主机向Botmaster传输盗取的信息。当用户从受感染的主机上传图像到Facebook时，僵尸会截取图像，并在发送到Facebook前使用YASS图像隐写技术将僵尸负载插入到图像中。当Botmaster准备发布命令时，它通过生成一个僵尸负载消息并将其上传至它的Facebook账户来完成，然而，图片占用很大的空间将显著增加僵尸网络信道的流量，容易被检测到。Stegobot图像隐写系统的结构如图3所示。

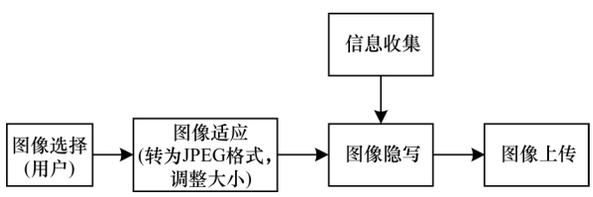

图3 Stegobot图像隐写系统

Fig.3 Stegobot image steganography system

3.2.2　基于文本隐写技术的社交僵尸网络

文献[3]介绍的DR-SNbot包括Botmaster、C&C-Server与Bot 3个部分。其中僵尸网络的控制端是Botmaster部分,这部分用来发送攻击命令。C&C-Server是命令控制服务器,是注册昵称对应的社交网络虚拟主机。每个C&C-Server对应进行一个企业不同的注册昵称,并将命令隐藏在僵尸网络日志中发布。当C&C服务器出现故障时,灾难恢复机器人会发出预警,通知攻击者构建新的C&C服务器,并自动修复C&C通信信道,以确保其强大的抗毁性。Bot是僵尸程序,通常运行在移动终端上,用于在C&C-Server上下载命令并解析执行这些命令。DR-SNbot的C&C信道命令的发布包括预处理、信息隐藏、POST、GET、信息提取、后处理6个步骤。预处理过程是指Botmaster对命令进行加密和签名,最终形成密文。信息隐藏是指Botmaster在一个属性域中隐藏一段密文,随后在正常日志中插入这个标签。这个被操作的属性域要拥有特殊的网页标签。僵尸主机通过HTTP的POST方式将日志上传到C&C-Server,Bot通过GET请求下载该日志,在Bot日志中寻找与众不同的网页标签(如<a>),确定该标签的属性域,并在提取信息隐藏阶段加密得到的密文。最后Bot验证Botmaster产生的数字签名,如果该签名验证最终是通过的,那么Bot对该消息进行解密,得到对应的明文(即命令),如果签名验证不通过,Bot会丢弃这条消息。C&C信道流程如图4所示。

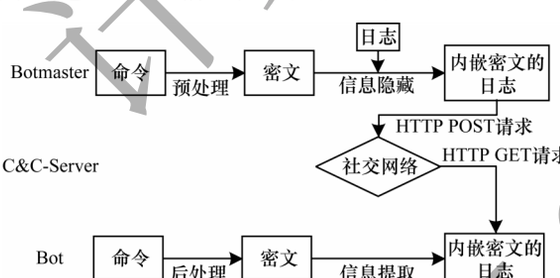

图4　DR-SNbot C&C信道流程

Fig.4　Procedure of DR-SNbot C&C channel

文献[4]介绍了将Twitter作为隐蔽的C&C信道的社交僵尸网络,它使用类似于文献[35]介绍的无噪声隐写技术。在这个系统中隐写对象是推文,秘密消息不包含在推文文本的数据中,而是包含在推文的元数据中(长度)。元数据是指“关于数据的数据”。所有数据都有一些与之相关的元数据,但是这个元数据并没有被详细地存储起来,它是从现有的数据推断出来的。推文的数据是文本,而这条推文还包含了一些元数据,比如发布的时间、用户的账号和发布的文本长度,额外的元数据还可以包括已发布文本的字母频率或文本中的空格数。该系统利用发布的推文的长度,通过一对多的字符计数设定编码规则来嵌入秘密消息。在发送命令时,首先将命令划分成为符号序列,结合预先设定的编码规则依次生成推文。然后每个秘密消息将按照原始秘密消息的顺序发布到Twitter账户。最后接收方的提取功能将按发布的(按时间顺序)顺序接收推文,并返回每个推文的长度值。解码函数可以应用与编码函数功能相同的映射,重构原始信息。隐蔽信道流程如图5所示。

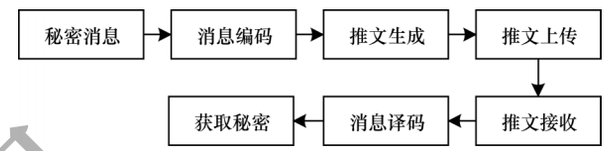

图5　基于Twitter的隐蔽C&C信道流程

Fig.5　Procedure of hidden C&C channel based on Twitter

基于文本隐写技术的社交僵尸网络还有文献[36]介绍的使用加密推文创建的僵尸网络C&C机制。这种方法是在包含僵尸网络命令的推文中混合不相关的句子。他们的命令推文遵循#keyword command的形式,其中command的值将被加密。虽然这种方法可以隐藏正在发出的command,但并不能隐藏command的存在。每个command遵循相同的形式,可以根据其他发布的推文将Botmaster账户区分出来。但是,如果由于检测到恶意活动而导致Botmaster的账户被禁用,则没有用于恢复的机制。文献[37]介绍的ELISABot使用Unicode隐写技术创建隐蔽C&C信道,将不可打印的字符注入到用户生成的内容中,避免了额外流量的产生。

3.3　社交僵尸网络发展趋势

随着社交网络在人类生活中作用的增大和网络技术的发展,社交僵尸网络也在不断发展。总体来讲,社交僵尸网络开始向高隐蔽、自动化的方向发展,同时其恶意行为也以虚假信息传播为主。为了避开用户行为特征和行为生物识别等传统社交僵尸网络检测方法,社交僵尸网络在逐渐提升其伪装程度,或是根据现有检测方法的原理对其模型进行调整,从而增大检测难度。同时,社交僵尸网络开始趋向于自动化运行。社交僵尸网络可以自动化地进行账户创建、模拟社交动作、执行社交网络平台的API等动作,从而提升了自身的工作效率。随着时间的推移,社交僵尸网络实现的主要目的从发送垃圾消息、窃取用户信息逐渐开始转向谣言散布、错假消息轰炸等。例如研究人员发现相当数量的社交僵尸网络被用来散布有关于疫苗效果的假消息[38]。同时,社交僵尸网络也被用于具有政治目的的舆论操控[39]。

4　社交僵尸网络检测

准确探测社交僵尸网络并对僵尸网络采取针对性遏制是打击僵尸网络犯罪的重要环节。因为社交僵尸网络不具备明显的恶意行为特征,所以无法针对社交僵尸网络的个体进行检测。相比而言,作为一个集合,社交僵尸网络表现出一些很独特的特征,这为其检测提供了思路。对于社交僵尸的检测,文

献[40-44]已经有了相应的介绍。从技术实现角度来看,社交僵尸网络检测一般分为针对服务器端的检测方法和针对主机端的检测方法。另外,针对近来出现的基于隐写技术的僵尸网络,研究人员根据图像与文本隐写技术的原理设计出了特定的检测方法。近年来,机器学习技术也提高了社交僵尸网络的检测效率,其与用户行为特征提取等传统检测方法的结合开始成为最新的研究热点。

4.1 服务器端检测方法

服务器端的检测方法一般是利用在线社交网络的用户信息[45-47],如用户发送的消息和好友请求等采用分类的方法来识别僵尸账户。近年来学术界对社交僵尸网络进行了研究,例如文献[48-51]介绍的社交僵尸网络特征发掘研究成果。

4.1.1 基于账户属性的社交僵尸网络检测

社交僵尸网络中的社交僵尸账户一般有如下群体属性:即注册时间集中、账户昵称相似、活跃时间集中和发送的推文内容或结构相似。这些特征都归结为使用自动或半自动工具在整个网络中操作大量的机器人账户,进而表现出了一些群体属性。基于这些群体属性,集合数据挖掘聚类算法,实现对社交僵尸网络的有效检测。文献[10]提出一种根据社交僵尸网络的群体特征的检测方法,通过注册时间集中、活跃时间集中、注册昵称相似等群体特征进行检测,检测流程如图6所示,其中,黑色圆圈代表僵尸账号,白色圆圈代表真实账号。

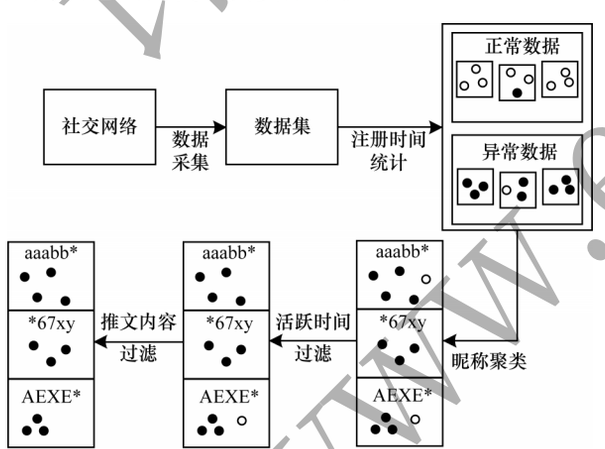

图6 社交僵尸网络检测流程

Fig.6 Procedure of social botnet detection

整个检测过程分为5步:1)采集大量来源于社交网络平台的数据,形成一个数据集;2)对数据分布集中度高的账号,提取账号的注册时间值进行统计,得到异常组;3)根据同一算法批量生成的僵尸账号昵称具备相似性的特点,采用K-Means聚类算法,结合注册时间异常组得到更进一步的异常组;4)对群组进行活跃时间过滤,排除真实账户;5)根据社交僵尸网络发送的推文内容一般在内容和结构上会具备一些相似性的特点,采用相似推文进行二次过滤,最终得到社交僵尸网络集合。

4.1.2 基于行为特征的社交僵尸网络检测

基于行为特征的社交僵尸网络检测主要是寻找社交僵尸存在的与普通账户在行为上的差异性,通过行为的相似度来聚类用户账户,从而发现类似行为的大量恶意账户。文献[52]使用人人网的数据集研究Sybils的链接创建行为、细粒度行为、群组之间的幕后串通行为,提出一个基于行为特征的Sybil账号的检测方法。文献[53]介绍了恶意账户在社交网络中松散的同步行为,基于这种行为特征可以通过聚类分析检测恶意账户。文献[54]提出的CatchSync可以用于查看有向图中节点的连通性,分析节点社交行为以发现可疑节点。

4.2 主机端检测方法

主机端的检测方法一般是通过检测主机一端的异常行为,如注册表修改、文件系统信息修改和系统调用来对社交僵尸网络进行检测。

4.2.1 基于行为生物识别的检测

基于行为生物识别技术的社交僵尸网络检测,主要是通过鼠标击键、键盘输入按键等特征来区分人类和社交僵尸。在访问社交网络的情况下,触发器通常是由用户引发的键盘或鼠标事件。然而,如果一个社交僵尸访问社交媒体来获取新的命令,或者上传获取的信息,那么是不需要通过用户事件触发的,而是由恶意软件的内部状态变化引起的。因此,社交僵尸和正常用户所表现出来的用户触发事件以及引发流量的原因就存在不同。文献[55-56]提出一种通过检测网络流量和用户事件之间的因果关系,从而检测社交僵尸网络形成的C&C流量的方法,如图7所示。研究人员通过检测输入按键、鼠标左键点击/释放、F5按键3个用户事件,区分正常用户和社交僵尸在社交网络流量上的不同。这种检测方法的缺点是上述的因果关系由于网络的延迟、操作系统本身的延迟和计算机性能差异等动态变化的因素,很难使得人类活动和网络流量完全同步,导致检测准确率降低。

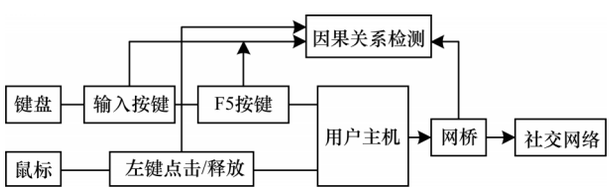

图7 基于行为生物识别的检测

Fig.7 Detection based on biological idetification

4.2.2 基于用户行为的检测

基于用户行为的检测主要是通过检测社交僵尸控制者在发布命令时与正常用户存在的行为方式上的差异[57]来检测社交僵尸网络。文献[58]提出一种在社交网络用户与相关内容中识别出垃圾邮件的方

法,他们发现一种非文本特征,这种特征只出现在垃圾邮件发送者的身上,并基于这种特征提出一种针对垃圾邮件的离线检测方法。文献[48]提出人类行为具有固定的伪周期性,与随机的行为混合在一起,几乎无法被模拟。因此,很容易将这种独特的人类行为与其他行为模式区分开来。通过分析社交网络中用户交互的不同尺度来区分正常用户和社交僵尸的特征行为,实现对社交僵尸网络的检测。文献[59]提出基于行为树的检测社交机器人的方法。在构建可疑行为树后,生成检测结果的模板库,通过模板和实际检测结果之间的匹配来检测社交僵尸网络。

近年来,社交僵尸网络开始运用隐写技术或其他较为新颖的加密方法,这导致基于服务器端和主机端的检测机制有时会失效,因此对于一些特定的社交僵尸网络还需要一些特定的检测方法。同时,在传统检测方法的基础上,研究人员开始引入机器学习技术来提升对社交僵尸网络的检测效果。

4.3　社交僵尸网络的特定检测方法

4.3.1　基于图像隐写技术的隐蔽型社交僵尸网络检测

对于基于图像隐写技术的隐蔽型社交僵尸网络Stegobot,文献[60]提出并设计一个检测方案,利用图像文件的信息熵作为检测的关注对象。该方案的检测技术实现了对几个不同的图像隐写技术方法的平均检测率超过70%。图像熵反映了图像的质量,图像的熵值定义为对像素信息不确定度的数学期望。每个像素表示一个事件,而图像则是像素的集合。图像熵之所以可以起到重要作用的关键原因在于,僵尸在对图像嵌入二进制文件前后,图像的熵值会发生显著的变化。由于嵌入技术将改变像素的概率分布以及封面图像的颜色信息,因此这些嵌入技术将改变图像的熵值。

文献[61]提出并设计了专门用于检测基于图像隐写系统的社交网络僵尸网络C&C信道的检测系统SocialClymene。文献[62]利用基于离散余弦变换的特征研究了Stegobot的检测方法。离散余弦特征对嵌入图像的变换十分敏感,可以提高识别图像的隐藏信息的检测率。离散余弦变换可以提供有用的特征来区分不同大小的正常和恶意的图像。

文献[63]利用文献[64-65]介绍的多媒体图像的内容特征、文献[66-68]介绍的用户属性的特征以及文献[69]介绍的社交图理论特征来识别用户行为,采用传统分类算法对Stegobot的可疑行为进行检测。

4.3.2　基于文本隐写技术的隐蔽型社交僵尸网络检测

对于基于文本隐写技术的隐蔽型僵尸网络DR-SNbot和文献[4]介绍的利用Twitter作为隐蔽的C&C信道的社交僵尸网络,伪随机别名是基于自定义算法动态生成的,可用于注册C&C服务器,具有较强的抗破坏性能。然而,运用同一算法生成的基于伪随机的僵尸用户的昵称与合法昵称相比,存在着较大的词法差异[70]。这种差异往往体现在两个昵称中出现频率较高的子串之间分布特征的差异。因此,文献[2]提出一种利用僵尸昵称的检测算法来检测此类社交僵尸网络。该算法主要由采集模块、挖掘模块、学习模块和检测模块4个部分构成。采集模块直接在现有的社交网络平台上收集正常用户的合法昵称样本,同时基于昵称生成算法产生大量僵尸昵称样本。这两类样本被随机分配到训练样本集和测试样本集中,其中训练集用于昵称可信度阈值的学习,测试集则用于研究方法有效性的验证。通过频繁子串挖掘分析算法[71],挖掘模块在合法的训练样本集中提取出一张频率数据表(称为频率表),其内容包括样本中频率最高的不同长度的子串以及它们对应的出现次数。随后,挖掘模块将该频率表发送给学习模块。学习模块基于阈值学习算法,使用这张表进行训练,最终得出昵称可信度的阈值。检测系统模块则对测试集中的数据进行分类,计算测试样本的可信度,根据学习模块得到的阈值将这些样本分为合法昵称和僵尸昵称两种。

4.3.3　基于机器学习的社交僵尸网络检测

近年来,研究人员开始将人工智能中的机器学习算法运用在社交僵尸网络的检测中,解决了上述的传统检测方法出现的一些问题。文献[72]设计一种基于半监督学习的社交僵尸网络检测系统SocialbotHunter。该检测系统将用户的社交圈和行为特征作为一个属性来看待,首先根据从用户的行为特征中抽取出的特征向量计算初始可疑分数,随后将所有用户的行为特征引入到一个马尔科夫随机域中,最后在域中引入置信传播算法来修正可疑分数,从而寻找到社交僵尸网络账号。这种方法不仅能解决传统的社交僵尸网络检测方法中出现的无法检测到高伪装程度的僵尸账号的问题,还具有良好的通用性,可以在Twitter及类似于Twitter的社交平台上实现较高的检测效率。文献[73]利用深度学习算法对基于行为特征的社交僵尸网络检测算法进行了优化。首先建立一张用户信任权图,并分析不同用户之间包括兴趣、URL、社交行为在内的用户行为的相似性。随后利用传统的社交僵尸网络检测算法将正常用户与僵尸用户区分开来。最后将上述算法的分类结果作为输入,使用深度神经网络的自动编码器来更加细致地对僵尸用户进行分类。相比于传统检测算法,深度学习检测算法在两个Twitter数据集上都得到了更高的检测准确率与更加细致的分类结果。

4.4　社交僵尸网络检测方法对比分析

下文对上述社交僵尸网络的检测方法的优缺点进行分析。社交僵尸网络的检测方法的主要分类如表2所示,主要分为服务器端检测方法、主机端检测

方法、基于隐写技术的检测方法以及机器学习检测方法4种。

表2 Socialbot检测机制

Table 2 Socialbot detection mechanisms

分类	检测方法	主要检测原理
服务器端检测	基于账户属性的检测	账户属性分析
	基于行为特征的检测	差异行为分析
主机端检测	基于行为生物识别的检测	生物特征监测
	基于用户行为的检测	人机特征区分
基于隐写技术的检测	基于图像隐写技术的检测	图像熵监测
	基于文本隐写技术的检测	频繁子串分析
基于机器学习的检测	—	神经网络分类

服务器端检测方法的主要优点是设计思路较为简单,选用的分类算法也较为传统。该检测方法的缺点在于社交网络中庞大的用户群体与用户动作数量会增大研究人员的工作量。另外,僵尸网络操纵者会尽量修正社交僵尸账户的群体特征以及与正常用户之间的行为差异,使其更加贴近于正常用户的对应特征。这会导致这种检测方法的失效,而这一问题会被基于机器学习的社交僵尸网络检测方法在一定程度上解决。

主机端的检测方法能够充分利用人与机器的不同点,对正常账户与社交僵尸账户进行较为有效的分类。主机端社交僵尸网络检测方法的缺点是社交僵尸在终端主机上只执行一些特定的活动,而且许多技术复杂度较高的社交僵尸网络不会在正常用户进行活动之前先进行恶意的活动,使得恶意活动与良性的用户活动混合在一起,加大了检测的难度。

相比于传统的检测方法,4.3节提及的两种基于隐写技术的社交僵尸网络检测方法能够有效地检测运用隐写技术的僵尸网络。但是,目前在图像隐写社交僵尸网络的研究成果都是在对一种隐蔽型社交僵尸网络(Stegobot)进行检测,对其他图像隐写社交僵尸网络缺乏足够的实验数据证明其有效性。同时,部分检测方法还存在针对文件较小的僵尸网络内置的恶意软件检测率较低[60]和假阳性率较高[61]的问题。对于文本隐写社交僵尸网络的检测也存在着类似的问题,研究人员多数只是对某一种社交僵尸网络进行特征分析和检测。总之,现存的隐写社交僵尸网络的检测方法缺少较为通用的检测方法,而且现有的特定检测方法还存在有待解决的问题。

目前出现的基于机器学习的社交僵尸网络检测方法能够在一定程度上解决服务器端与主机端检测方法中出现的通用性差、检测算法复杂等问题[70],同时也能够进一步提升社交僵尸网络检测的性能上限。然而,这种检测方法的性能会受到诸如用户行为特征等预定义属性的选取的影响[74],即研究人员选择不同的用户行为特征会导致不同的检测结果。这种特征选取的过程是十分耗时的,明显增加了研究人员的工作量,从而导致这一检测方法虽然在一定程度上提升了检测准确率,但却增加了相当的时间成本。另外,基于机器学习的检测方法需要对社交僵尸网络的特征有较为深入的了解,因此对于未知的或新型的社交僵尸网络,机器学习方法难以进行有效的检测。最后,还要注意到机器学习技术对于硬件具有一定的要求,这也是限制基于机器学习的社交僵尸网络检测方法普遍使用的原因之一。

5 社交僵尸网络接管与反制

在社交僵尸网络的检测方法上如何实现对社交僵尸网络的反制也是加强社交网络平台防护的关键。如果能获取现有社交僵尸网络的控制权,实现社交僵尸网络的接管,研究人员就能够更加深入地研究社交僵尸网络的工作机制,从而能够提升社交网络平台对僵尸网络的防护水平。目前,尚无发现社交平台上的僵尸网络的反制与接管技术的研究,本文参考针对其他类型的僵尸网络的接管与反制技术的研究,给出了社交僵尸网络在这两方面的未来发展方向。

5.1 社交僵尸网络的反制技术发展方向

目前,研究人员提出了一些具有一定通用性的僵尸网络反制方案,主要包括蜜罐方法、网络限制与数据包分析方法、基于群体驱动的方法以及其他方法等。

近年来研究人员开始在研究僵尸网络时引入蜜罐技术,实现对僵尸网络的检测和数据的收集。文献[75]提出一种基于CVE-2017-17215漏洞的中交互蜜罐系统。这一蜜罐系统通过模拟不安全的SOAP服务来实现远程代码注入漏洞,其主要分为核心模块、服务模块、进程模块、监控模块4个模块。其中主模块对于上述的漏洞进行了模拟,服务模块提供了蜜罐系统的控制界面,进程模块实现了对于控制界面的操作,监控模块则用来监视蜜罐的工作状态。文献[76]提出一种极有创造力的蜜罐设计方案。该方案通过模拟僵尸网络的一个被感染的节点,来直接与僵尸网络的C&C服务器进行连接,从而误导服务器来向蜜罐系统发出命令和通信。基于这种思路,研究人员设计出由传统的被动式蜜罐、解释器、主动型蜜罐和STIX解释器组成的僵尸网络蜜罐系统。其中被动式蜜罐用来进行僵尸网络的捕获,解释器用来分析被动式蜜罐收集到的恶意软件样本,STIX解释器则用来将其他3个模块的数据进行解释与存储。对于社交僵尸网络而言:一种研究方向是模拟一个被感染的僵尸用户来连接到社交僵尸网络的命令控制服务器上;另一种研究方向则是通过模拟社交僵尸网络的命令控制服务器来误导僵尸用户与其进行连接。

网络限制与数据包分析的反制方法是指在检测僵尸网络的基础上,通过限制IP地址与数据包的方法阻断僵尸网络的运行与规模扩大。文献[77]提出一种以自治系统为单位的社交僵尸网络反制方法。其中,每个自治系统存储主机IP地址列表和每个主机的阈值,并将其分别存入“黑名单”、“白名单”、“潜在攻击者”与“潜在僵尸主机”4类。自治系统通过区块链相连,并每20 s更新一次阈值来确保安全防护更新到最新。文献[78]提出一种基于流量的僵尸网络防护方案。该方案通过分析监控网络中交换机的数据包传输速度的变化来区分僵尸网络流量与正常流量,并对僵尸网络流量的数据包进行阻断。对于社交僵尸网络,研究人员需要与社交网络平台合作,实现对于平台内流量的分析、检测与选择性阻断。

基于群体驱动的反制方法是指在设计僵尸网络检测系统的基础上开放其源码,使得全球的技术人员都可以对该程序进行修改与完善,这样能够集合团体的力量提升僵尸网络检测系统的有效性[79]。对于社交僵尸网络来讲,研究人员也可以采取类似的方法,从而实现对社交僵尸网络尤其是新型的社交僵尸网络的有效检测。

其他的方法还包括僵尸节点清除技术、数据污染技术等[80]。对于社交僵尸网络来讲,研究人员可以与社交网络平台合作,设计对于僵尸用户的特征分析与清除方案,也可以通过对各种类型的社交僵尸网络的命令控制信道的原理进行分析,实现对僵尸网络命令的污染,从而达成破坏僵尸网络正常运作的目的。

5.2　社交僵尸网络的接管方法发展方向

从近年来的研究来看,僵尸网络的接管技术存在着较大的研究空白。其中,最有参考价值的是文献[8]提出的对于Torpig僵尸网络的接管方法。该方法利用Torpig僵尸网络通过域名确定C&C服务器的特点,使用域名生成算法生成了两个僵尸网络认定为C&C服务器的域名。在僵尸主机尝试连接这两个域名时,研究人员设计给予僵尸主机以对应的响应,从而误导僵尸主机错将其认定为本应连接并传输其具体信息的C&C服务器,最终获取这一僵尸网络10天的控制权,并在这10天内收集到了近70 GB的流量数据和近10 GB的Apache日志文件数据。针对前文所述的社交僵尸网络,研究人员也可以采取类似的思路尝试进行接管,即通过模仿C&C服务器的行为,迷惑僵尸主机使其连接到研究人员预先设定的服务器上。这种方法的重点在于需要对僵尸网络服务器的工作原理有着深入的了解。

6　研究现状及未来展望

6.1　已有研究存在的问题

在社交僵尸网络的C&C信道预测方面,已有的工作大多存在实现过程复杂、可用性差的缺点,且无法跨终端平台实现与管控。

在社交僵尸网络检测方面,以主机端检测和服务器端检测为主流研究方向,但已有成果大多存在检测性能差、通用性差的问题,且检测多是针对某一特定平台进行,无法做到跨平台检测。基于用户属性的检测方法,由于分词系统存在误差,在聚类时有些类似的昵称可能会被划分到不同的簇,导致原本不同的簇可能会属于同一个社交僵尸网络,而且这种方法无法实现实时对社交僵尸网络的在线检测。对于基于用户行为的检测,随着社交僵尸网络模仿正常用户行为能力的提高,检测难度在不断增大,检测的性能和准确性要求也变得难以达到。基于隐写技术的检测和基于机器学习的检测方法都缺乏通用性。同时,基于机器学习的技术对于硬件与对社交僵尸网络的了解程度要求较高。

在社交僵尸网络对抗方面,目前存在法律监管、威胁情报共享等非技术难题,需要全球范围内有关机构和平台进一步重视社交僵尸网络问题,形成基于高效率协作的应对机制。

6.2　未来研究方向

综合上述的分析讨论和社交僵尸网络当前的发展态势,未来社交僵尸网络领域的研究重点包括:1)深入研究社交僵尸网络所利用的逃避机制,寻找社交僵尸网络共同的特征;2)分析社交僵尸网络C&C信道的隐蔽方式,研究相应的检测和防御方法;3)研究社交僵尸网络对抗机制,实现跨平台关联与管控,减少社交僵尸网络的危害;4)运用机器学习技术,在传统检测方法的基础上进一步提升社交僵尸网络检测方法的效率;5)在检测的基础上进一步研究如何能够遏制僵尸网络的恶意行为,例如尝试接管僵尸网络,或者部署针对僵尸网络的反制措施;6)结合相关法律法规的制定,对社交僵尸网络进行溯源,打击其幕后的控制者,尝试从根本上减少社交僵尸网络的产生。

7　结束语

随着社交网络的发展,社交僵尸网络成为僵尸网络的重要分支。本文介绍了僵尸网络的概念与发展现状以及现有的社交僵尸网络的基本特征,总结当前社交僵尸网络的检测方法并展望了接管与反制技术的未来发展方向。考虑到目前社交网络的爆炸式发展与区块链、隐写、人工智能等新技术的出现,研究人员需要对不同类型的社交僵尸网络进行深入分析,研究设计具有通用性与高效性的社交僵尸网络信道检测方法。通过设计跨平台的社交僵尸网络对抗机制,协同各安全厂商、社交平台和监管部门共同应对社交僵尸网络的威胁,在有效检测的基础上,尝试从技术角度遏制社交僵尸网络的恶意行为,并通过立法打击幕后黑手。

参考文献

[1] 伍静,詹千熠,刘渊. 一种结合文本情感分析的微博僵尸粉识别模型[J]. 计算机工程,2020,46(6):288-295.
WU J,ZHAN Q Y,LIU Y. A zombie fans recognition model for microblog combining text sentiment analysis[J]. Computer Engineering,2020,46(6):288-295. (in Chinese)

[2] NAGARAJA S,HOUMANSADR A,PIYAWONGWISAL P,et al. Stegobot:a covert social network botnet[C]//Proceedings of IEEE International Conference on Information Hiding. Washington D. C. ,USA:IEEE Press,2011:299-313.

[3] YIN T,ZHANG Y Z,LI S H. DR-SNBot:a social network-based botnet with strong destroy-resistance[C]//Proceedings of the 9th IEEE International Conference on Networking,Architecture,and Storage. Washington D. C. ,USA:IEEE Press,2014:191-199.

[4] PANTIC N,HUSAIN M I. Covert botnet command and control using Twitter[C]//Proceedings of the 31st Annual Computer Security Applications Conference. New York,USA:ACM Press,2015:171-180.

[5] 诸葛建伟,韩心慧,叶志远,等. 僵尸网络的发现与跟踪[C]//2005年全国网络与信息安全技术研讨会论文集. 北京:[出版者不详],2005:1-7.
ZHUGE J W,HAN X H,YE Z Y,et al. Discovery and tracking of botnets[C]//Proceedings of 2005 National Symposium on Network and Information Security Technology. Beijing:[s. n.],2005:1-7. (in Chinese)

[6] 张治起. 僵尸网络命令控制信道研究[D]. 北京:北京邮电大学,2012.
ZHANG Z Q. Research on command and control channel of botnet[D]. Beijing:Beijing University of Posts and Telecommunications,2012. (in Chinese)

[7] HOLZ T,GORECKI C,FREILING F,et al. Detection and mitigation of fast-flux service networks[C]//Proceedings of the 15th Annual Network and Distributed System Security Symposium. Washington D. C. ,USA:IEEE Press,2008:2268-2277.

[8] STONE-GROSS B,COVA M,CAVALLARO L,et al. Your botnet is my botnet:analysis of a botnet takeover[C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. New York,USA:ACM Press,2009:635-647.

[9] CUI X,FANG B X,YIN L H,et al. Andbot:towards advanced mobile botnets[C]//Proceedings of the 4th USENIX Conference on Large-scale Exploits and Emergent Threats. [S. 1.]:USENIX Association,2011:1-11.

[10] MENDES L D P,ALOI J,PIMENTA T C. Analysis of IoT botnet architectures and recent defense proposals[C]//Proceedings of the 31st IEEE International Conference on Microelectronics. Washington D. C. ,USA:IEEE Press,2019:186-189.

[11] KAMBOURAKIS G,KOLIAS C,STAVROU A. The mirai botnet and the IoT zombie armies[C]//Proceedings of IEEE Military Communications Conference. Washington D. C. ,USA:IEEE Press,2017:267-272.

[12] BALLANO M. Is there an Internet-of-things vigilante out there[EB/OL]. [2021-03-10]. https://community. broadcom. com/symantecenterprise/communities/community-home/librarydocuments/viewdocument? DocumentKey=ef23b297-5cc6-4c4a-b2e7-ff41635965fe&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

[13] ALI S T,MCCORRY P,LEE P H J,et al. ZombieCoin:powering next-generation botnets with bitcoin[C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin,Germany:Springer,2015:34-48.

[14] FRANZONI F,ABELLAN I,DAZA V. Leveraging bitcoin testnet for bidirectional botnet command and control systems[C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin,Germany:Springer,2020:3-19.

[15] Socialbot[EB/OL]. [2021-03-10]. https://en. wikipedia. org/wiki/Social_bot.

[16] 倪平,张玉清,闻观行,等. 基于群体特征的社交僵尸网络检测方法[J]. 中国科学院大学学报,2014,31(5):691-700,713.
NI P,ZHANG Y Q,WEN G X,et al. Detection of socialbot networks based on population characteristics[J]. Journal of University of Chinese Academy of Sciences,2014,31(5):691-700,713. (in Chinese)

[17] GRIZZARD J B,SHARMA V,NUNNERY C,et al. Peer-to-peer botnets:overview and case study[C]//Proceedings of HotBots'07. New York,USA:ACM Press,2007:1-8.

[18] RATKIEWICZ J,CONOVER M,MEISS M,et al. Truthy:mapping the spread of Astroturf in microblog streams[C]//Proceedings of the 20th International Conference Companion on World Wide Web. Washington D. C. ,USA:IEEE Press,2011:249-252.

[19] DICKERSON J P,KAGAN V,SUBRAHMANIAN V S. Using sentiment to detect bots on Twitter:are humans more opinionated than bots?[C]//Proceedings of 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. New York,USA:ACM Press,2014:620-627.

[20] ABOKHODAIR N,YOO D,MCDONALD D W. Dissecting a social botnet:growth,content and influence in Twitter[C]//Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing. New York,USA:ACM Press,2015:839-851.

[21] TANNER B K,WARNER G,STERN H,et al. Koobface:The evolution of the social botnet[C]//Proceedings of 2010 eCrime Researchers Summit. Washington D. C. ,USA:IEEE Press,2010:1-10.

[22] BOSHMAF Y,MUSLUKHOV I,BEZNOSOV K,et al. Design and analysis of a social botnet[J]. Computer Networks,2013,57(2):556-578.

[23] 何毓锟. 社交网络僵尸研究[D]. 长春:吉林大学,2015.
HE Y K. Research on bot of social networks[D]. Changchun:Jilin University,2015. (in Chinese)

[24] CALLADO A,KELNER J,SADOK D,et al. Better network traffic identification through the independent combination of techniques[J]. Journal of Network and Computer

Applications,2010,33(4):433-446.
[25] KARTALTEPE E J,MORALES J A,XU S H,et al. Social network-based botnet command-and-control: emerging threats and countermeasures[C]//Proceedings of ACM Conference on Applied Cryptography and Network Security. New York,USA:ACM Press,2010:511-528.
[26] 李跃,翟立东,王宏霞,等. 一种基于社交网络的移动僵尸网络研究[J]. 计算机研究与发展,2012,49(S2):1-8.
LI Y,ZHAI L D,WANG H X,et al. Mobile botnet based on SNS[J]. Journal of Computer Research and Development,2012,49(S2):1-8. (in Chinese)
[27] ZeroFox Research. Inside the massive SIREN social networkspam botnet[EB/OL]. [2021-03-10]. https://www.zerofox.com/blog/inside-massive-siren-social-network-spam-botnet/.
[28] SINGH A,TODERICI A H,ROSS K,et al. Social networking for botnet command and control[J]. International Journal of Computer Network and Information Security,2013,5(6):11-17.
[29] GAO J,LIU M. A study on social network based P2P botnet[J]. Science,2017,2(3):204-208.
[30] JSteg[EB/OL]. [2021-03-10]. http://zooid.org/~paul/crypto/jsteg/.
[31] SOLANKI K,SARKAR A,MANJUNATH B S. YASS:yet another steganographic scheme that resists blind steganalysis[C]// Proceedings of International Workshop on Information Hiding. Berlin,Germany:Springer,2007:16-31.
[32] SALLEE P. Model-based methods for steganography and steganalysis[J]. International Journal of Image and Graphics,2005,5(1):167-189.
[33] PROVOS N. Defending against statistical steganalysis[EB/OL]. [2021-03-10]. https://hdl.handle.net/2027.42/107890.
[34] WESTFELD A. F5-A steganographic algorithm[C]//Proceedings of the 4th International Workshop on Information Hiding. Berlin,Germany:Springer,2001:289-302.
[35] DESOKY A. Noiseless steganography:the key to covert communications[M]. [S.1.]:CRC Press,2012.
[36] SEBASTIAN S,AYYAPPAN S,VINOD P. Framework for design of Graybot in social network[C]//Proceedings of 2014 International Conference on Advances in Computing,Communications and Informatics. Washington D.C.,USA:IEEE Press,2014:2331-2336.
[37] COMPAGNO A,CONTI M,LAIN D,et al. Boten ELISA:a novel approach for botnet C&C in online social networks[C]// Proceedings of 2015 IEEE Conference on Communications and Network Security. Washington D.C.,USA:IEEE Press,2015:74-82.
[38] BRONIATOWSKI D A,JAMISON A M,QI S H,et al. Weaponized health communication:Twitter bots and Russian trolls amplify the vaccine debate[J]. American Journal of Public Health,2018,108(10):1378-1384.
[39] LUCERI L,DEB A,GIORDANO S,et al. Evolution of bot and human behavior during elections[J]. First Monday,2019,24(9):1-29.
[40] VERKAMP J P,MALSHE P,GUPTA M,et al. Facebot:an undiscoverable botnet based on treasure hunting social networks[EB/OL]. [2021-03-10]. http://research.jverkamp.com/.
[41] CHU Z,GIANVECCHIO S,KOEHL A,et al. Blog or block:detecting blog bots through behavioral biometrics[J]. Computer Networks,2013,57(3):634-646.
[42] YAN G H. Peri-watchdog:hunting for hidden botnets in the periphery of online social networks[J]. Computer Networks,2013,57(2):540-555.
[43] XUE J L,YANG Z,YANG X Y,et al. VoteTrust:Leveraging friend invitation graph to defend against social network Sybils[C]//Proceedings of IEEE INFOCOM'13. Washington D.C.,USA:IEEE Press,2013:2400-2408.
[44] FERRARA E,VAROL O,DAVIS C,et al. The rise of social bots[J]. Communications of the ACM,2016,59(7):96-104.
[45] XIA H,LI L,CHENG X G,et al. Modeling and analysis botnet propagation in social Internet of things[J]. IEEE Internet of Things Journal,2020,7(8):7470-7481.
[46] TAN E H,GUO L,CHEN S Q,et al. Spammer behavior analysis and detection in user generated content on social networks[C]//Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems. Washington D.C.,USA:IEEE Press,2012:305-314.
[47] CHU Z,GIANVECCHIO S,WANG H N,et al. Detecting automation of Twitter accounts:are you a human,bot,or cyborg?[J]. IEEE Transactions on Dependable and Secure Computing,2012,9(6):811-824.
[48] BRITO F,PETIZ I,SALVADOR P,et al. Detecting social-network bots based on multiscale behavioral analysis[C]// Proceedings of IEEE International Conference on Emerging Security Information,Systems,and Technologies. Washington D.C.,USA:IEEE Press,2013:4578-4586.
[49] GAO H Y,HU J,WILSON C,et al. Detecting and characterizing social spam campaigns[C]//Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement. New York,USA:ACM Press,2010:35-47.
[50] CAO L,QIU X F. ASP2P:an advanced botnet based on social networks over hybrid P2P[C]//Proceedings of the 22nd Wireless and Optical Communication Conference. Chongqing,China:[s.n.],2013:677-682.
[51] FAGHANI M R,NGUYEN U T. Socellbot:a new botnet design to infect smartphones via online social networking[C]// Proceedings of the 25th IEEE Canadian Conference on Electrical and Computer Engineering. Washington D.C.,USA:IEEE Press,2012:1-5.
[52] YANG Z,WILSON C,WANG X,et al. Uncovering social network Sybils in the wild[J]. ACM Transactions on Knowledge Discovery from Data,2014,8(1):1-29.
[53] CAO Q,YANG X W,YU J Q,et al. Uncovering large groups of active malicious accounts in online social networks[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York,USA:ACM Press,2014:477-488.
[54] JIANG M,CUI P,BEUTEL A,et al. CatchSync:catching synchronized behavior in large directed graphs[C]// Proceedings of the 20th ACM SIGKDD International

Conference on Knowledge Discovery and Data Mining. New York, USA: ACM Press, 2014: 941-950.
[55] BURGHOUWT P, SPRUIT M, SIPS H. Towards detection of botnet communication through social media by monitoring user activity[C]//Proceedings of International Conference on Information Systems Security. Berlin, Germany: Springer, 2011: 131-143.
[56] JI Y D, HE Y K, JIANG X Y, et al. Combating the evasion mechanisms of social bots[J]. Computers and Security, 2016, 58: 230-249.
[57] 徐华露,汤娟,刘嘉勇. 基于随机森林的微博僵尸账号检测研究[J]. 现代计算机,2020(30):16-20.
XU H L, TANG J, LIU J Y. Research on detecting zombie accounts using random forest[J]. Modern Computer, 2020(30): 16-20. (in Chinese)
[58] TAN E H, GUO L, CHEN S Q, et al. Spammer behavior analysis and detection in user generated content on social networks[C]//Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2012: 305-314.
[59] JI Y D, HE Y K, JIANG X Y, et al. Towards social botnet behavior detecting in the end host[C]//Proceedings of the 20th IEEE International Conference on Parallel and Distributed Systems. Washington D. C., USA: IEEE Press, 2014: 320-327.
[60] NATARAJAN V, SHEEN S N, ANITHA R. Detection of StegoBot: a covert social network botnet[C]//Proceedings of the 1st International Conference on Security of Internet of Things. Washington D. C., USA: IEEE Press, 2012: 36-41.
[61] GHANADI M, ABADI M. SocialClymene: a negative reputation system for covert botnet detection in social networks[C]// Proceedings of the 7th International Symposium on Telecommunications. Washington D. C., USA: IEEE Press, 2014: 954-960.
[62] FRIDRICH J, GOLJAN M, HOGEA D. Steganalysis of JPEG images: breaking the F5 algorithm[C]//Proceedings of International Conference on Information Hiding. Berlin, Germany: Springer, 2002: 310-323.
[63] VENKATACHALAM N, ANITHA R. A multi-feature approach to detect stegobot: a covert multimedia social network botnet[J]. Multimedia Tools and Applications, 2017, 76(4): 6079-6096.
[64] KODOVSKY J, FRIDRICH J, HOLUB V. Ensemble classifiers for steganalysis of digital media[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 432-444.
[65] NATARAJAN V, ANITHA R. Universal steganalysis using contourlet transform[M]. Berlin, Germany: Springer, 2012.
[66] FIRE M, KATZ G, ELOVICI Y. Strangers intrusion detection-detecting spammers and fake proles in social networks based on topology anomalies[EB/OL]. [2021-03-10]. https://www. researchgate. net/publication/258513228.
[67] NATARAJAN V, SHEEN S N, ANITHA R. Multilevel analysis to detect covert social botnet in multimedia social networks[J]. The Computer Journal, 2014, 58(4): 679-687.
[68] SAKAKI T, OKAZAKI M, MATSUO Y. Earthquake shakes Twitter users: real-time event detection by social sensors[C]//Proceedings of the 19th International Conference on World Wide Web. Washington D. C., USA: IEEE Press, 2010: 851-860.
[69] TRACY E M, WHITTAKER J K. The social network map: assessing social support in clinical practice[J]. Families in Society: the Journal of Contemporary Social Services, 1990, 71(8): 461-470.
[70] YADAV S, REDDY A K K, REDDY A L N, et al. Detecting algorithmically generated malicious domain names[C]//Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement. New York, USA: ACM Press, 2010: 48-61.
[71] BORGELT C, KRUSE R. Induction of association rules: apriori implementation[M]. [S. 1.]: Physica-Verlag, 2002.
[72] DORRI A, ABADI M, DADFARNIA M. SocialBotHunter: botnet detection in Twitter-like social networking services using semi-supervised collective classification[C]//Proceedings of the 16th IEEE International Conference on Dependable, Autonomic and Secure Computing. Washington D. C., USA: IEEE Press, 2018: 496-503.
[73] LINGAM G, ROUT R R, SOMAYAJULU D, et al. Social botnet community detection: a novel approach based on behavioral similarity in Twitter network using deep learning [C]//Proceedings of the 15th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2020: 708-718.
[74] ABULAISH M, FAZIL M. Socialbots: impacts, threat-dimensions, and defense challenges[J]. IEEE Technology and Society Magazine, 2020, 39(3): 52-61.
[75] ZHANG W Z, ZHANG B, ZHOU Y, et al. An IoT honeynet based on multiport honeypots for capturing IoT attacks[J]. IEEE Internet of Things Journal, 2020, 7(5): 3991-3999.
[76] OLIVERI A, LAURIA F. Sagishi: an undercover software agent for infiltrating IoT botnets[J]. Network Security, 2019(1): 9-14.
[77] AHMED Z, DANISH S M, QURESHI H K, et al. Protecting IoTs from mirai botnet attacks using blockchains[C]// Proceedings of the 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks. Washington D. C., USA: IEEE Press, 2019: 1-6.
[78] YIN D, ZHANG L M, YANG K. A DDoS attack detection and mitigation with software-defined Internet of things framework[J]. IEEE Access, 2018, 6: 24694-24705.
[79] THANH VU S N, STEGE M, EL-HABR P I, et al. A survey on botnets: incentives, evolution, detection and current trends[J]. Future Internet, 2021, 13(8): 198.
[80] 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.
WANG T Z, WANG H M, LIU B, et al. Some critical problems of botnets[J]. Chinese Journal of Computers, 2012, 35(6): 1192-1208. (in Chinese)

编辑 索书志