移动僵尸网络研究与进展

徐 建,吴烨虹,程晶晶
(南京邮电大学 计算机学院,江苏 南京 210046)

摘 要:僵尸网络是计算机重要的安全威胁。随着智能终端的发展,这一安全威胁出现在移动设备平台上。在了解传统僵尸网络传播原理和控制方式的基础上,对移动僵尸网络的传播、命令控制机制以及控制协议进行了深入研究,并简单介绍了移动僵尸网络的危害以及对它的防御。移动僵尸网络主要是存在于移动设备上的僵尸网络,它是以一般的僵尸网络理论为基础,建立的一种新型的网络攻击形式。而且今后移动僵尸网络将会严重影响人们的生活。因此必须不断地分析和掌握在不同网络环境下的命令控制协议,保证每个用户都能远离网络攻击的威胁。

关键词:移动僵尸网络;蓝牙;无线网络;命令控制
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2015)05-0118-05
doi:10.3969/j.issn.1673-629X.2015.05.028

Research and Development of Mobile Botnets

XU Jian, WU Ye-hong, CHENG Jing-jing
(College of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210046, China)

Abstract: Botnet is an important threat on computer security. As the development of mobile terminals, the security threat rises on mobile device platforms. Based on understanding the traditional Botnet propagation principle and control mode, the spread of mobile Botnet and command and control mechanisms and control protocol are studied in-depth, also introduce the hazards and its defense of mobile Botnet briefly. Mobile Botnet is mainly existed in a Botnet on a mobile device, which is a new form of network attack established based on the general theory of the Botnet. In the future, mobile Botnet will seriously affect the people's life. Therefore must constantly analyze and grasp C&C protocol in different network environment, ensuring that each user can be far away from the threat of cyber attacks.

Key words: mobile Botnet; Bluetooth; WiFi; C&C

0 引 言

僵尸网络是个人 PC 机在网络中最严重的安全威胁之一。僵尸网络是攻击者利用各种手段传播僵尸程序,将大量主机感染成僵尸主机,并通过命令与控制信道操纵这些僵尸主机,实施分布式拒绝服务攻击、垃圾邮件发送以及敏感信息窃取等恶意行为的网络[1]。但是在移动环境下,来自于僵尸网络的威胁还不是很多。近年来,随着大量智能手机的发展,例如:Iphone、安装了安卓系统的手机等,移动终端和设备的攻击数量和复杂度在不断提高。近几年里,智能手机发展非常迅猛。大多数智能手机上都安装了具有多功能的操作系统,比如 Linux, Windows Mobile, Android 以及 Symbian OS。安装了系统的智能手机在运行环境中越来越近似于 PC 机,在智能手机中存储了更多的个人信息和重要数据,通过网络下载安装了许多应用。随着用户数据量的不断增长和第三方应用的分享,使得智能手机很容易遭受到恶意软件的攻击。由于现在的智能手机被作为了网络终端,PC 机提供的一些服务,在与智能手机相类似的智能终端上都可以享受到,比如现在比较流行的支付宝、余额宝以及银行一些服务等。但是智能终端并没有 PC 机那样安全的保护措施,从另一方面也引诱了犯罪。现在已经发现在安卓市场存在大量的恶意软件应用。虽然应用在安装之前,安卓平台也需要身份验证,但它所设定的策略不严格,允许开发者签署他们自己的应用,以此攻击者很容易将恶意软件上传到安卓市场。而 Iphone 应用市场控制的就比较严格,但是对于已经“越狱”的苹果产品,可以安装任何应用,并在后台运行进程,这就失去了苹果公司

收稿日期:2014-07-03 **修回日期**:2014-10-08 **网络出版时间**:2015-04-22
基金项目:国家自然科学基金资助项目(61202353);江苏省高校自然科学研究资助项目(12KJB520008)
作者简介:徐 建(1980-),男,硕士,工程师,研究方向为信息安全、人工智能。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150422.1005.015.html

所给予的安全。

智能手机无论是从它的计算能力,还是它所拥有的功能,某种程度上都在慢慢地代替 PC 机的使用。但是它在处理事务的同时也失去了安全和个人隐私的保护。现如今专门针对移动终端的攻击越来越复杂。在 2004 年出现了第一个概念验证(botnet-esque)手机蠕虫病毒 Cabir,从它的出现找到了移动恶意软件的转化过程。早期的恶意软件只是感染文件,更改系统的一些应用,发送 SMS/MMS 消息,通常一个恶意软件只有一两个功能。尽管近年来,移动恶意软件的数量以及它们的变体都在增长,但到目前为止,它们的功能仍然还很简单。直到 2009 年 2 月发现了 SymbOS. Exy. A[2]木马程序,随即在 2009 年的 7 月再次出现它的变体 SymbOS. Exy. C[3]。从此以它为代表的移动僵尸网络呈现出快速发展的趋势。一旦被感染,它会连接回一个恶意的 HTTP 服务器,报告服务以及用户的相关信息。在 2009 年 11 月出现的 Ikee. B[4]蠕虫病毒,它的目标就是"越狱"的 Iphone,行为类似于 SymbOS. Exy。Ikee. B 也是通过 HTTP 连接到控制服务器下载额外的组件并发送回用户的信息。通过远程链接,攻击者周期性地发出指令来调整被感染的设备,发动大规模的攻击。在 2011 年 3 月,从安卓市场清除出 50 多个包含一种叫"Droid Dream"恶意软件的应用。这种恶意软件可以非法获得 root 权限,窃取用户的敏感信息,建立僵尸网络。在 2012 年 2 月,在中国的第三方应用程序市场出现的 RootSmart[5],它连接了成千上万的安卓设备,形成了僵尸网络。一旦启动,RootSmart 将连接到远程服务器发送感染手机的各种信息,并获取 root 权限,从而从服务器获取手机升级的特权。在用户不知道的情况下,控制被感染的手机发送额外的 SMS 信息,并使用其他额外的电话增值服务。由于这种恶意软件本身并不含有任何恶意代码,因此让 Bouncer 也很难侦测。从僵尸主控端高额的利润回报来看,移动僵尸网络将成为智能手机最严重的威胁。文中详细介绍了移动僵尸网络的传播途径、命令控制机制以及危害。

1　移动僵尸网络概述

1.1　移动僵尸网络的定义

移动僵尸网络(mobile botnet)通过网络蠕虫、后门技术、蓝牙技术、SMS、MMS 和 WiFi 等技术和应用,传播移动僵尸程序并控制大量智能终端设备,形成具有隐蔽性的一对多的命令与控制网络。参阅传统僵尸网络的定义,这里给出了移动僵尸网络的定义[6-7]:移动僵尸网络是指攻击者针对智能手机和移动互联网,出于恶意目的,借鉴传统僵尸网络技术并利用一对多的命令与控制信道组成的网络。

1.2　移动僵尸网络的特点

尽管各个智能终端、移动设备与普通计算机之间有着硬件和软件的差别,但在主要功能模块上还是相通的,因此移动僵尸网络和传统僵尸网络具有很多相似之处[8]。常见的计算机恶意软件可以直接对移动僵尸网络产生威胁,然而它也有自己的特点。

(1)传染性。

由于不同的厂商会安装不同的操作系统,因此移动僵尸网络要针对某一系统编写僵尸程序,放在没有经过安全认证的应用商店、手机论坛上的应用软件里,供人们下载。还通过利用蓝牙、WiFi、SMS 等方式进行传播。在"刷机"的过程中,也会受到感染。

(2)破坏性。

传统恶意软件只是破坏计算机的软件和硬件设备,而移动僵尸网络还可以窃取隐私数据,恶意扣费等。

(3)资源有限性。

类似于智能手机的移动终端设备受到自身电池带电量的限制,它在通信过程中,不断地消耗电量。随着网络通信的增加,也加大了对网络数据资费的加大。

(4)网络连通性不稳定。

由于移动设备自由度比较高,它的使用不一定以同一个方式连入网络。智能手机可以通过 WiFi、2G\3G\4G 等方式连入网络,而且不同的网络稳定性也存在差异。

(5)IP 地址。

在移动僵尸网络间连接时,会因 IP 地址的缺乏出现问题,大部分的手机都是使用 NAT 网关的,这使得基于 IP 地址的命令与控制网络不适合移动僵尸网络。

(6)潜伏性。

当移动僵尸网络相关的恶意软件在智能终端上成功安装之后不会立即发作,它会隐藏其僵尸程序安装的痕迹,删除安装包,并蛰伏在终端上。在适当的时间段与特定服务器进行通信,根据设定好的运行周期或利用用户的空闲时间发作。

(7)寄生性。

很多僵尸网络的程序是寄生在一些热门应用软件里。当用户在没有认证的机制的应用商店或论坛上下载安装时,也许恶意软件已经被你触发。通过用户连入网络再传播出去。

2　移动僵尸网络的传播方式

移动僵尸网络的传播方式多种多样。它继承了传统的下载式传播和电脑连接式传播。文中详细介绍具有移动特点的几种传播方式。

2.1 蓝牙传播

近年来,基于蓝牙的恶意软件被大家广泛关注。入侵者利用被盗用的手机,使用蓝牙搜索附近的设备,和别的设备配对成功后,会试图把他们的恶意软件注入到周边的移动手机用户。Su Jing 等[9]提出在蓝牙协议的实现中,存在一组不同的已知安全漏洞,他们认为这种漏洞的存在,再加上蓝牙复杂度的说明及其大型的代码库,将针对使用蓝牙通道的用户,采取更复杂的攻击。例如:Cabir、Mabir、Commwarrior 的蠕虫都是利用了这个漏洞。移动手机僵尸网络通过蓝牙来传播控制消息与基于 P2P 网络的僵尸网络非常相似。它们有一个共同的特点:即使防御者识别了僵尸网络的一部分,那剩下的僵尸网络也不会被破坏。它们与集中的方式(如 IRC)相比,没有固定的僵尸主控机发送命令。对于蓝牙僵尸网络,任意的蓝牙设备都可以充当僵尸主控机发出消息,这样不确定的僵尸主控机设备也可以有效地逃避检测。此外蓝牙僵尸网络也有它本身的特性吸引着僵尸网络创造者,就是它的距离,是在一定距离允许范围内实现设备之间的通信。所以恶意软件通过蓝牙来传播需要两个条件:首先通过蓝牙通信需要在一定的范围之内,而且需要开启蓝牙功能;其次移动终端需要感染了病毒(安装了病毒文件)。因此从以上条件来看,以蓝牙作为传播手段不会出现病毒大规模爆发的情况。但如果处在手机密集的公共场所中,在蓝牙的通信范围之内,那感染病毒的智能手机就会大幅增加,所以蓝牙还是一种传播病毒的载体。蓝牙手机病毒的传播不是集中式的,它是攻击者与受害者之间的暂时性连接,使得其很难被监控并给出合理的防治措施[10]。

2.2 WiFi 传播

相对于其他的通信媒介,WiFi 网络具有一定的优势,可以用于建立移动僵尸网络。虽然前面所介绍的蓝牙也可以建立移动僵尸网络,但由于受到范围和传输率的限制,而且它也不能作为垃圾邮件或 DDOS 攻击的媒介。相比之下,无线僵尸网络可以实现更快的传输速度,支持多种僵尸网络活动,范围可以分散到多个城市。对于加密的或封闭的网络来说,无线僵尸网络如果想入侵就比较困难,因此无线僵尸网络只有利用开放的和未加密的无线网络。在家庭的 WiFi 网络不想被别人占用,基本上都是加密的,安全性受到大家的重视,而一些公共场所(如餐馆、咖啡馆)却都是开放的和非加密的。一般开放的无线网络的商家都是通过 80 端口来限定在线活动的网络流量。移动的 WiFi 僵尸网络使用了基于 HTTP 的控制命令信道,在它的流量中具有更好的隐蔽性,很容易被认为是安全网络。命令服务器一般会使用确定改变域名的新命令进行定期查询,移动僵尸网络还可以进一步提高它的隐蔽性,主要是通过限定其命令控制查询开放的无线网络。

假设在开放的无线网络环境下,所有的设备都感染了相同的僵尸恶意软件,允许忽略不同设备感染的并发情况。当在家或者在办公室时,移动设备有充足的时间处在无线网络中,然而很少或没有研究能够确定僵尸网络活动可以只存在于开放的无线网络,它可以极大地阻碍检测。如果在一个单一的大城市里,在开放的无线网络里存在一个小型的移动僵尸网络,面对防御者的威胁,僵尸主机需要达到三个目标。首先僵尸机在最大瞬间和高速时期能够足够多地控制整个僵尸网络的一部分,但是这样的控制比较难。可以通过设计和模拟一个命令控制协议来实现这一目标。在平时的上班时间以及周末,考虑在这些不同的时间段,获得实际属于僵尸网络的数量,以及僵尸机频繁地接收命令和新命令在整个僵尸网络中的传播速度。第二个目标是使用小型移动无线僵尸网络成功地发出 DDOS 攻击。同样,也可以设计和模拟这样的攻击行为。最终目标是僵尸网络 C&C 和 DDOS 攻击可以在一种隐蔽的方式下进行,通过确保恶意僵尸网络的流量是充分分散在多个无线接入点[11]。

2.3 SMS/MMS 传播

智能手机在平时的使用中,以高频率使用 SMS/MMS 来发送消息[12]。往往在这些消息中嵌入式链接指向包含有恶意代码的虚拟主机,一般没有足够的注意和警告的用户很可能因为好奇会去点击那些下载恶意程序的链接。相对于 SMS 来说,MMS 能提供更多元化的移动通信服务,在传输的信息中包括了图像、视频等一些多媒体信息,因此利用 MMS 传播恶意软件更受到入侵者的青睐。在 2005 年发现的第一个通过 MMS 传播的 Symbian 蠕虫 Commwarrior. A,同时也通过蓝牙传播。当用户被此病毒感染后,它会自动复制拷贝,并从被感染的手机通讯录中选择发送目标,将复制的病毒程序隐藏在 MMS 的 SIS 文件中发送出去。一般含有病毒的 MMS 都具有诱惑性的标题,引诱用户来点击,从而使接收者感染。以前纯文本的 SMS 服务具有以下的局限性:首先受到消息长度的限制,信息产业部在《点对点短信息协议》中规定每条短信的最大长度是 140 个字节或 70 个字符。若每次发送短信超过 70 个汉字,系统会将其自动分为多条信息来发送;其次信息的形式单一,SMS 只支持简单的文本形式,不能集成图像及音频信息。且传输速率低,由于 SMS 使用速率很低的信令信道,使得传输率较低,等待时间较长。

由于现在智能手机支持 TCP/IP 协议栈,所以也可通过网络浏览和 Email 的方式受到僵尸程序的感染。随着智能终端的发展,它的功能不断加强,更多基于计

算机的传统僵尸网络的传播和控制技术将会被应用到移动僵尸网络。因此在未来将会有更多的移动僵尸网络出现。

3　移动僵尸网络的命令控制机制

所谓移动僵尸网络的命令控制机制主要是指通过 C&C 信道传输僵尸主控机的控制命令及数据,并可以与受控的僵尸机进行通信。控制命令机制包括了通信的协议、拓扑结构以及所使用的软件资源等。

方滨兴等在文献[13]中提到僵尸网络的拓扑结构可分为中心结构、P2P 结构、组合结构和混合结构。纯中心结构的僵尸网络如图 1 所示,僵尸网络控制者通过控制僵尸网络的中心节点以达到操控整个僵尸网络的目的。在早期的僵尸网络是采用 IRC 和 HTTP 来构成中心结构的僵尸网络;而在移动网络中是可以通过群发短信的方式构建基于 SMS 控制的中心结构移动僵尸网络。

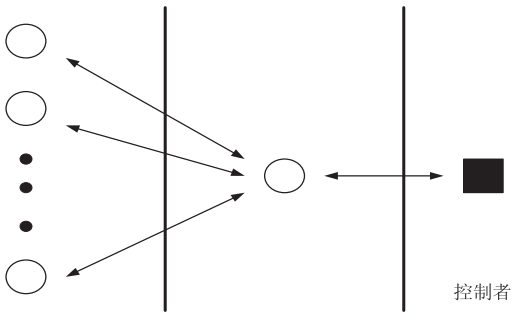


图 1　纯中心结构僵尸网络图

但是在所建立中心结构的僵尸网络很容易被防御者破坏,这是由于所有的指令和数据都是由位于中心节点的僵尸主控机发出,防御者只需要破坏僵尸主控机,整个僵尸网络就会瘫痪,这就是所说的“斩首行动”[14]。因此之后产生了 Domain Flux 技术,如图 2 所示。通过一个动态可变的中心服务器群来控制僵尸网络,这使得防御者很难找到僵尸主控机的所在。

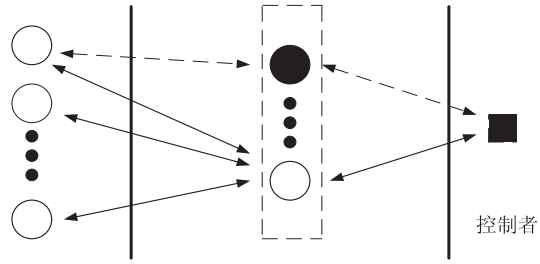


图 2　基于 Domain Flux 技术的中心结构僵尸网络图

纯 P2P 僵尸网络结构如图 3 所示。主要采用点对点的模式,每个僵尸节点同时充当僵尸主机的角色,因此纯 P2P 僵尸网络并不存在专用的僵尸主控机,并不依赖于某一个节点。在移动网络中通过 SMS 通信机制同样可以建立纯 P2P 结构的移动僵尸网络,可以在每个移动终端设置转发命令的僵尸网络通信录列表来达到转发的效果,从而建立纯 P2P 结构的僵尸网络。

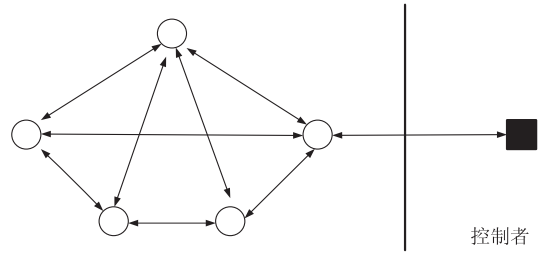
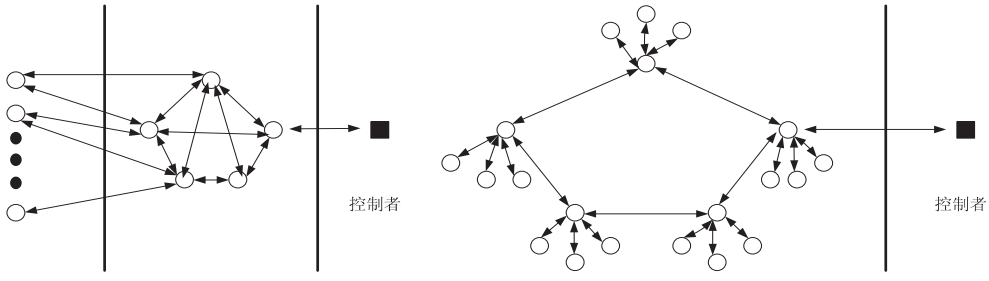


图 3　纯 P2P 结构僵尸网络图

组合结构的僵尸网络如图 4 所示。



(a) 中心结构为主　　(b) P2P结构为主

图 4　组合结构僵尸网络图

组合结构包括了两种情况:

(1)以中心结构为主的僵尸网络,它的僵尸主控机不是一个,是由 P2P 结构的网络组成,形成一个动态控制服务器群。所谓动态就是通过不确定地访问僵尸主控机群中的僵尸主控机来接受控制命令和数据。

(2)以 P2P 结构为主的僵尸网络,它的僵尸主控机仍然是由 P2P 结构组成,但从同样规模的僵尸网络中其数量远远大于前者,在 P2P 结构中的每一个僵尸主控机又是一个中心结构的通信机制。

从以上的分析得出,组合结构不仅吸取了纯中心结构和纯 P2P 结构的优点,还消除了两者的缺点,它是由僵尸主控机的控制者可以自由定义的高级 C&C 协议。但是现在如何将这一结构应用于移动僵尸网络,还处于理论研究阶段,在某些方面的设计还需要进一步的思考。

混合结构就是采用上述结构的两种或两种以上进行组合,来增强命令控制信道的容灾性及可生存性。像 Conficker 就同时使用 Domain Flux 和 Random 协议,

当 Domain Flux 失效后,启动 Random 协议实现命令控制,增加健壮性。

4 结束语

僵尸网络作为当今最具威胁的网络攻击计算平台,攻击手段多种多样,例如分布式拒绝服务攻击、垃圾邮件、网络钓鱼、点击欺诈或隐私窃取等等。它感染移动终端的最终目的就是获得利益,具有移动僵尸网络特色的攻击包含:恶意扣费、隐私信息窃取、垃圾短信干扰、电量消耗、网络流量消耗、DDOS 攻击等。由于现在的智能手机功能不断地增多,许多都涉及到个人的银行账户,多数功能都与经济挂钩,因此也诱导了不法分子不断地建立新的网络攻击行为。因此要警惕乱码的电话,不接收陌生短信,不接受陌生的网络连接请求,不在手机上浏览陌生网站和邮件,经常给手机杀毒,安装手机防火墙,等等。

参考文献:

[1] 王海龙,唐 勇,龚正虎. 僵尸网络命令与控制信道的特征提取模型研究[J]. 计算机工程与科学,2013,35(2):62-67.

[2] SymbOS. Exy. A[EB/OL]. 2009. http://www.symantec.com/security_response/writeup.jsp? docid=2009-022010-4100-99.

[3] Asrar I. Could sexy space be the birth of the sms botnet? [EB/OL]. 2009-07-13. http://www.symantec.com/connect/blogs/could sexy space be birth sms botnet.

[4] Porras P, Saidi H, Yegneswaran V. An analysis of the Ikee. B Iphone Botnet[C]//Proc of MOBISEC. Berlin: Springer, 2010:141-152.

[5] RootSmart[EB/OL]. 2012-02-03. http://www.csc.ncsu.edu/faculty/jiang/RootSmart/.

[6] 耿贵宁. 移动僵尸网络安全分析关键技术研究[D]. 北京:北京邮电大学,2012.

[7] 诸葛建伟,韩心慧,周勇林,等. 僵尸网络研究[J]. 软件学报,2008,19(3):702-715.

[8] 刘一静,孙 莹,蔺 洋. 基于手机病毒攻击方式的研究[J]. 信息安全与通信保密,2007(12):96-98.

[9] Su Jing, Chan K K W, Miklas A G, et al. A preliminary investigation of worm infections in a bluetooth environment[C]//Proc of ACM workshop on recurring malcode. Alexandria, VA: ACM, 2006.

[10] Singh K, Sangal S, Jain N, et al. Evaluating bluetooth as a medium for botnet command and control[C]//Proc of the 7th international conference on detection of intrusions and malware, and vulnerability assessment. Berlin: Springer, 2010:61-80.

[11] Knysz M, Hu Xin, Zeng Yuanyuan, et al. Open WiFi networks: lethal weapons for botnets? [C]//Proc of the 31st annual IEEE international conference on computer communications. [s.l.]: IEEE, 2012:2631-2635.

[12] 王 畅,戴 航,孙启禄. 智能手机上僵尸网络综述[J]. 微处理机,2012,33(2):39-44.

[13] 方滨兴,催 翔,王 威. 僵尸网络综述[J]. 计算机研究与发展,2011,48(8):1315-1331.

[14] 李 跃. 面向移动网络的僵尸网络关键技术研究[D]. 成都:西南交通大学,2013.

(上接第 117 页)

Barbara, CA, USA: [s.n.], 2005:36-54.

[3] 葛伟平,汪 卫,周皓峰,等. 基于隐私保护的分类挖掘[J]. 计算机研究与发展,2006,43(1):39-45.

[4] 路慧萍,童学锋. 保持隐私的决策树生成过程研究[J]. 计算机应用,2005,25(6):1382-1384.

[5] Jha S, Kruger L, Daniel P M. Privacy preserving clustering [C]//Proceedings of the 10th European symposium on research in computer security. Milan, Italy: [s.n.], 2005:397-417.

[6] Vaidya J, Clifton C. Privacy-preserving k-means clustering over vertically partitioned data[C]//Proceedings of the eleventh ACM SIGKDD international conference on knowledge discovery in data mining. Washington DC, USA: ACM, 2008:206-215.

[7] 张国荣,印 鉴. 分布式环境下保持隐私的聚类挖掘算法[J]. 计算机工程与应用,2007,43(18):165-167.

[8] 姚 瑶,吉根林. 一种基于隐私保护的分布式聚类算法[J]. 计算机科学,2009,36(3):100-102.

[9] 雷红艳,邹汉斌. 限制隐私泄露的隐私保护聚类算法[J]. 计算机工程与设计,2010,31(7):1444-1446.

[10] Clifton C, Kantarcioglu M, Vaidya J. Defining privacy for data mining[C]//Proceedings of the national science foundation workshop on next generation data mining. Baltimore, MD, USA: [s.n.], 2002:126-133.

[11] Kantarcioglu M, Clifton C. Privacy preserving distributed mining of association rules on horizontally partitioned data[J]. IEEE Transactions on Knowledge and Data Engineering, 2004,16(9):1026-1037.

[12] 宋宝莉,覃 征. 分布式环境下关联规则的安全挖掘算法[J]. 计算机工程,2006,32(21):35-37.

[13] 黄毅群,卢正鼎,胡和平,等. 分布式环境下保持隐私的关联规则挖掘算法[J]. 计算机工程,2006,32(13):12-14.

[14] Samet S, Miri A. Privacy preserving protocols for perception learning algorithm in neural networks[C]//Proceedings of the 4th IEEE international conference on intelligent systems. Varna, Bulgaria: IEEE, 2008:1065-1070.

[15] Yang Zhiqiang, Wright R N. Privacy-preserving computation of Bayesian networks on vertically partitioned data[J]. IEEE Transactions on Knowledge and Data Engineering, 2006, 18(9):1253-1264.

移动僵尸网络研究与进展

作者： 徐建， 吴烨虹， 程晶晶， XU Jian， WU Ye-hong， CHENG Jing-jing
作者单位： 南京邮电大学 计算机学院,江苏 南京,210046
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(5)