计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2016.20160419
53(10):2189-2206,2016

僵尸网络发展研究

李 可[1,2] 方滨兴[1,4] 崔 翔[1,2,3] 刘奇旭[2,3]
[1](北京邮电大学 北京 100876)
[2](中国科学院信息工程研究所 北京 100097)
[3](中国科学院大学 北京 101408)
[4](东莞电子科技大学电子信息工程研究院 广东东莞 523808)
(like_bupt@foxmail.com)

Study of Botnets Trends

Li Ke[1,2], Fang Binxing[1,4], Cui Xiang[1,2,3], Liu Qixu[2,3]
[1](*Beijing University of Posts and Telecommunications*, *Beijing*, 100876)
[2](*Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing*, 100097)
[3](*University of Chinese Academy of Sciences*, *Beijing*, 101408)
[4](*Institute of Electronic and Information Engineering*, *Dongguan University of Electronic Science and Technology of China*, *Dongguan*, *Guangdong*, 523808)

Abstract Botnets, as one of the most effective platforms to launch cyber-attacks, pose great threats to the security of today's cyber-space. Despite the fact that remarkable progress had been made in the researches of botnets' both attack and defense technologies in recent years, the forms and command and control mechanisms of botnets, however, as Internet applications are put into a wider variety of uses and communication technologies upgraded more rapidly than ever, are also undergoing constant changes, bringing new challenges to defenders. For this reason, an in-depth investigation of botnets' working mechanisms and development is of great significance to deal with the threats posed by botnets. This paper, with the attack technologies of botnets as its main focus, gives an comprehensive introduction of the working mechanisms of botnets in terms of its definition, transmission, lifecycle, malicious behaviors and command and control channels, and divides the botnets' development into two stages, namely, attacks to traditional PC and extensive attacks, with the technological features, behavioral characteristics, case studies and evolutionary patterns of each stage elaborated in a detailed manner. After a summary of existing work on the defense of botnets with the limitations of each approach discussed, possible future attempts are presented.

Key words botnet; command and control channel (C&C channel); countermeasure; value-added network attack; survey

摘 要 僵尸网络(botnet)作为最有效的网络攻击平台,给当今互联网安全带来了巨大威胁.虽然近几年关于僵尸网络的攻防技术研究取得了显著进展,然而,伴随着互联网应用的多元化以及通信技术的不断革新,僵尸网络的形态和命令控制机制也在不断发生变化,这给防御人员带来了新的挑战.深入了解僵尸网络运行机理和发展趋势对有效应对僵尸网络引发的安全威胁具有重要意义.以僵尸网络攻击技术为核心,从形式化定义、传播方式、生命周期、恶意行为、命令控制信道方面对僵尸网络机理进行全面

收稿日期:2016-06-14;**修回日期**:2016-08-11
基金项目:国家自然科学基金项目(61303239);广东省产学研合作项目"广东省健康云安全院士工作站"(2016B090921001)
This work was supported by the National Natural Science Foundation of China (61303239) and the Industry-University-Research Cooperation Project of Guangdong Province (2016B090921001).

介绍,按时间顺序将僵尸网络的发展历程划分为 PC 攻击和广泛攻击 2 个阶段,对各阶段的技术特点、行为特性、代表案例以及演化规律进行详细阐述,总结当今僵尸网络防御方法和研究成果,对已有研究遗留的问题和未来可能研究热点进行讨论.

关键词 僵尸网络;命令控制信道;网络对抗;增值网络攻击;综述

中图法分类号 TP393

僵尸网络(botnet)被广泛认为是在传统蠕虫、木马、后门工具的基础上融合形成的复杂的网络攻击形式之一,是一种通过入侵网络空间内若干非合作用户终端构建的、可被攻击者远程控制的通用计算平台[1].其中,被入侵的用户终端称之为僵尸主机(bot)或者"肉鸡";攻击者指对僵尸网络具有实际操控权的控制者(botmaster).通过命令控制信道(command and control channel, C&C channel),攻击者可以一对多地操控僵尸主机发起恶意软件分发、垃圾邮件、DDoS、钓鱼攻击、用户身份窃取、点击欺诈、虚拟货币挖掘、加密勒索[2]等攻击活动.

出于利益目的,攻击者以僵尸网络为攻击发起平台,通过网络犯罪牟利,严重侵害互联网用户的隐私和财产安全.围绕其危害性,国内外媒体出现过大量相关报道.2011 年出现的 ZeuS GameOver 僵尸网络在全球范围内累计感染了约 100 万台主机,通过窃取用户银行账户信息和加密勒索方式,非法牟利超过 1 亿美元[3].赛门铁克发布的年度互联网安全威胁报告[4]指出 2013 年全球每天产生约 290 亿封垃圾邮件,其中有 76%来源于僵尸网络.2015 年一季度卡巴斯基在全球范围内共监测 23 095 起由僵尸网络发起的 DDoS 攻击,其中中国遭受了 8 553 起 DDoS 攻击,在 76 个受攻击国家中排名第一[5].根据 CNCERT 发布的 2016 年 3 月互联网安全威胁报告显示,我国木马或僵尸程序控制的主机 IP 数达到 196 万,环比上涨 44.9%.赛门铁克 2016 年 5 月发表的安全威胁报告显示[6],2015 年我国僵尸主机数量占到全球总量 46.1%,利用肉鸡发起的恶意活动同比上升 84%.

2002 年出现的 Agobot 引发了人们对于僵尸网络的关注,在此之后僵尸网络成了安全领域研究人员探讨的热点话题.国际学术组织举办专门的研讨会议对此问题进行探讨:ACM 协会从 2003 年开始举办的 WORM 会议(Workshop on Rapid Malcode)以僵尸网络为重要议题;USENIX 协会从 2007 年开始举办了僵尸网络专题研讨会 HotBots(Workshop on Hot Topics in Understanding Botnets);2008 年,WORM 与 HotBots 合并为 LEET(Workshop on Lager-scale Exploits and Emergent Threats),专门探讨僵尸网络、间谍软件和蠕虫.国际僵尸网络对抗联盟 AILB-IBFA 从 2013 年 12 月起举办专题研讨会议 BotConf,围绕最新僵尸网络发展态势和防御研究成果展开讨论.近几年 IEEE S&P, CCS, NDSS, Usenix Security 等国际顶级安全会议上也相继发表了有关论文[7-11],为僵尸网络研究提供了新思路.

僵尸网络作为一种高级形态的恶意代码,具有影响范围广、破坏性强、控制机制复杂、灵活多变的特性,给传统的安全防御方法带来了巨大的挑战,研究人员需对其演化过程以及发展趋势进行全面了解.近几年,伴随着攻防博弈的不断升级、互联网新兴技术的普及,僵尸网络在形态、命令控制机制、恶意行为方面发生了重大变化,而国内外尚缺少僵尸网络演化的系统性介绍.因此,深入理解僵尸网络工作原理和关键技术、总结当前僵尸网络新特性和演化规律对于开展僵尸网络防御工作具有重要意义.

基于上述事实,本文主要以僵尸网络近几年的发展趋势和攻防技术演化为核心内容,从僵尸网络的定义、命令控制、传播途径、恶意行为和生命周期 5 个方面对僵尸网络工作机制进行阐述;深入探讨僵尸网络的 PC 攻击阶段和广泛攻击 2 个发展阶段的演化过程和阶段特性;同时从防御角度出发,对主流僵尸网络防御方法进行总结归纳.

1 僵尸网络机理特性

僵尸网络在具备传统恶意代码部分特性的同时又有其独有特点,充分理解其机理特性是深入开展相关研究的重要前提.国内外相关综述类文献对该部分内容有过介绍[1,12-14],本文从僵尸网络的定义和范畴界定出发,关注其本质和工作机理,围绕僵尸网络传播、恶意行为、生命周期以及命令控制信道展开描述.

1.1　僵尸网络定义

1.1.1　僵尸网络形式化定义

定义 1. 僵尸网络. 僵尸网络由四元组所构成,反映可被攻击者通过命令控制信道进行远程控制使之进入特定状态的计算机群. 记为 $Botnet=(Zombie, Botmaster, CMD, CCC)$:

1) *Zombie*. 攻击者通过入侵手段获取的僵尸主机集合,记为 $Zombie=(BOT, S, Activity)$. 其中,$BOT$ 表示运行在受控僵尸主机上的僵尸程序集合,记为 $BOT=\{bot_1, bot_2, \cdots, bot_n\}$,$n$ 反映了该僵尸网络的规模;S 代表僵尸程序状态集合;$Activity$ 代表僵尸程序接受指令后执行的动作集合.

为了实现攻击能力和利益最大化,攻击者对感染的僵尸主机环境和性能有一定要求[15],可归纳为 5 个方面:

① 可用性. 指僵尸主机长时间在线、可通过命令控制信道正确接受攻击指令或进行信息回传的能力,这是僵尸主机最基本的能力要求.

② 生存性. 指僵尸程序在受害主机环境中的存活能力,不同终端类型僵尸网络所面临的生存挑战存在差异. 例如,在 PC 僵尸网络中,僵尸主机的生存威胁主要来自杀毒软件和防火墙等防护措施;而对于移动僵尸网络,其生存性还需要考虑资费和电量消耗的问题[16].

③ 计算性能. 指僵尸主机的 CPU 或者 GPU 的运算能力,该属性可帮助攻击者实现复杂的数据处理. 例如攻击者可以利用高运算能力的僵尸主机进行比特币挖掘[17].

④ 网络资源. 包含 IP 地址、地理位置、带宽、域名等资源. 大量覆盖全球范围的僵尸主机资源可克服时区和局部网络访问限制,为攻击者提供长期稳定的业务能力.

⑤ 内容资源. 指僵尸主机所包含的有价值信息,一般包含邮箱账户、银行账户、联系人等个人隐私信息,攻击者获取这些信息后可发起恶意推广、金融账户窃取、电话诈骗等攻击.

2) *Botmaster*. 指僵尸网络控制者,通过命令控制信道操纵僵尸主机群执行恶意活动.

3) *CMD*. 是僵尸程序可执行的控制命令集合. 记为 $CMD=\{cmd_1, cmd_2, \cdots, cmd_n\}$,常见的命令可分为更新和攻击两大类.

4) *CCC*. 是僵尸网络命令控制信道,该部分是整个僵尸网络实现的基础与核心,进一步可用形式化定义为 $CCC=(TOPOLOGY, PROTOCOL, RESOURCE, METHOD)$

① *TOPOLOGY*,僵尸网络命令控制信道拓扑结构.

② *PROTOCOL*,僵尸网络信道协议集合,包含 IRC, HTTP, Kademilia, Domian-Flux, Fast-Flux, Tor, SMS 等.

③ *RESOURCE*,控制者使用的软件和服务资源集合,包括域名、密钥、代理节点、跳板网络、公共服务、P2P 网络节点等.

④ *METHOD*,命令控制过程中涉及的关键算(方)法,涵盖 C&C 服务器寻址方法、认证机制、加密和编码算法 3 部分.

1.1.2　僵尸网络范畴界定

僵尸网络作为一种由恶意代码演化的命令驱动型攻击平台,通常被反病毒厂商归为蠕虫、后门、间谍软件以及木马的范畴,未能给出准确的定义和区别. 如图 1 和表 1 所示,1)僵尸网络包含的僵尸程序属于恶意代码范畴,具备恶意软件的部分特征;2)僵尸网络包含特有的一对多命令控制信道,这也是僵尸网络与传统恶意代码的最大区别[18].

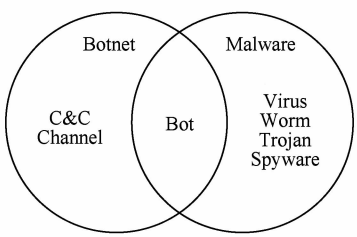


Fig. 1　Relationship between the Botnet and malwares.

图 1　僵尸网络与传统恶意代码关系

Table 1　Comparison between the Botnet and Malwares

表 1　僵尸网络与恶意代码关系

Category	Independence	Spread	Controllability	Information Steal	Collaborative
Botnet	Yes	Optional	Yes	Optional	Yes
Virus	No	Passive	No	No	No
Worm	Yes	Active	No	No	No
Trojan	Yes	Generally not	Yes	Yes	No
Spyware	Yes	Generally not	No	Yes	No

① 病毒(Virus)是通过感染计算机程序进行传播的恶意代码,必须具备感染性,且自身是一段代码而非独立程序,不可作为进程独立运行,而僵尸程序可以(且多数)不具备感染文件的能力.

② 蠕虫(Worm)是一种可自我复制的恶意代码,必须具备自动传播能力,而僵尸程序可以不具备自传播能力,其传播可通过社会工程学的方法实现.

③ 间谍软件(Spyware)是在未经用户明确授权的情况下窃取用户信息的恶意代码.因此,间谍软件必须具备窃密功能,而僵尸网络窃密功能是可选的.

④ 木马(Trojan)是与僵尸程序最接近的恶意代码,两者的关系一直具有争议性,本文认为二者具有3方面的差异:Ⅰ控制方式的差异.木马控制者在使用木马时,一定要在线;而僵尸网络控制者在使用僵尸网络过程中,可以离线.Ⅱ协同性差异.木马之间一般不强调协同工作,而僵尸网络则经常需要协同完成任务,比如命令中继、DDoS攻击等.Ⅲ功能差异.当前主流的木马通常具有屏幕监控、摄像头监测、文件管理等功能,而僵尸程序一般不具备这些功能.

1.2 僵尸网络传播机制

僵尸网络的构建依赖入侵脆弱主机并植入僵尸程序,该过程通常称为僵尸程序传播,或者称为僵尸网络招募.早期僵尸程序的传播以远程漏洞攻击、弱口令扫描入侵、文件共享和U盘传播方式为主.

近年来,随着防御机制的不断完善,原有传播方法难以达到理想效果.攻击者开始采用邮件附件、网页挂马(drive-by-download)、应用软件捆绑、付费安装(pay-per-install)、中间人攻击(man-in-the-middle)等隐蔽的方式进行传播.例如,ZeroAccess[19]通过伪装成杀毒软件和序列号生成器诱骗用户安装;Koobface[20]利用受害者社交网站账号向其好友推送视频链接,诱骗用户安装恶意插件实现感染.

1.3 僵尸网络恶意行为

Grizzard等人[21]曾按照过程将恶意行为划分为信息散布(information dispersion)、信息收集(information harvesting)、信息处理(information processing)三个方面.如图2所示:

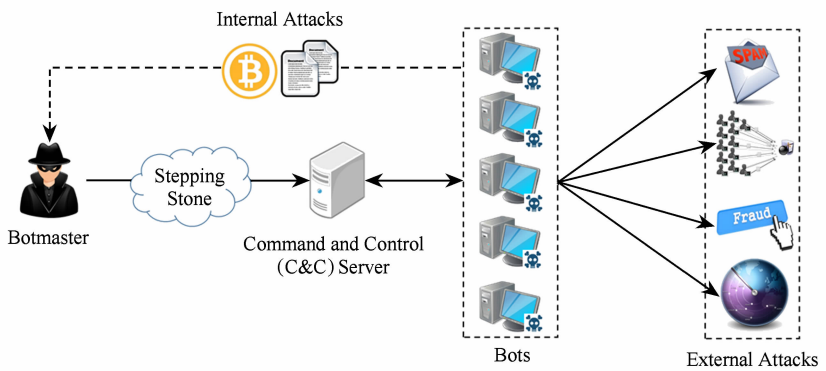


Fig. 2 Malicious behavior classification of botnets.

图2 僵尸网络恶意行为分类

从攻击作用点的角度将恶意行为归纳为2类:

1) 外部攻击.攻击者利用肉鸡带宽、CPU、IP等资源对外发动的网络攻击,攻击目标主要为互联网中其他用户和机构.DDoS、钓鱼攻击、垃圾邮件、点击欺诈、扫描等行为均属于该类.

2) 内部攻击.此类型攻击没有直接的外部攻击对象,其最大的受害者就是肉鸡本身,攻击者通过利用和挖掘肉鸡自身资源来牟利.常见的形式包括信息窃取、虚拟货币挖掘、加密勒索等.

除了上述方法外,一方面,攻击者可通过租赁服务(botnet-as-a-service)的方式牟利,根据趋势科技发布的中国地下网络犯罪调查报告显示[22],2014—2015年期间,每100台Windows 2003或2008系统的僵尸主机租赁价格约为24美元;另一方面,攻击者正在地下市场中出售ZeuS和Spyeye[23]等僵尸网络的攻击套件(crimeware rootkit),购买者可利用这些套件生成定制化的僵尸程序来感染更多脆弱主机,造成更为广泛的危害.

1.4 僵尸网络生命周期

已知研究将僵尸网络的生命周期定义为"从脆弱主机感染到成为活跃态的僵尸主机"[14],本文描述僵尸主机从传播到消亡过程的状态迁移,将典型的僵尸网络生命周期划分为"传播态"(spreading)、"工作态"(working)、"闲置态"(idle)、"离线态"(offline)、"隔离态"(block)和"消亡态"(dead)六个状态,状态的迁移变化如图3所示.

1) 新感染并运行的僵尸程序处于闲置态,此时僵尸程序试图获取控制命令;

2) 当获得传播命令(或默认自动传播)时,僵尸程序进入传播态,通过僵尸程序的传播,僵尸网络规模得到扩大;当获得其他命令时,僵尸程序进入工作态,执行命令完毕后转回到闲置态;

3) 当僵尸程序所在计算机或网络不可用时(如关机、休眠、断网等外力操作),僵尸程序转为离线态,离线态僵尸程序在有限时间内会恢复运行,并进入上述某种状态;

4) 当僵尸程序被外力隔离使之无法获取控制命令,则处于隔离态,隔离态僵尸程序无法正常工作.当外力撤销后,会转为传播、工作或闲置状态之一;

5) 僵尸程序被清除时,僵尸网络规模缩小,最终会进入消亡态.

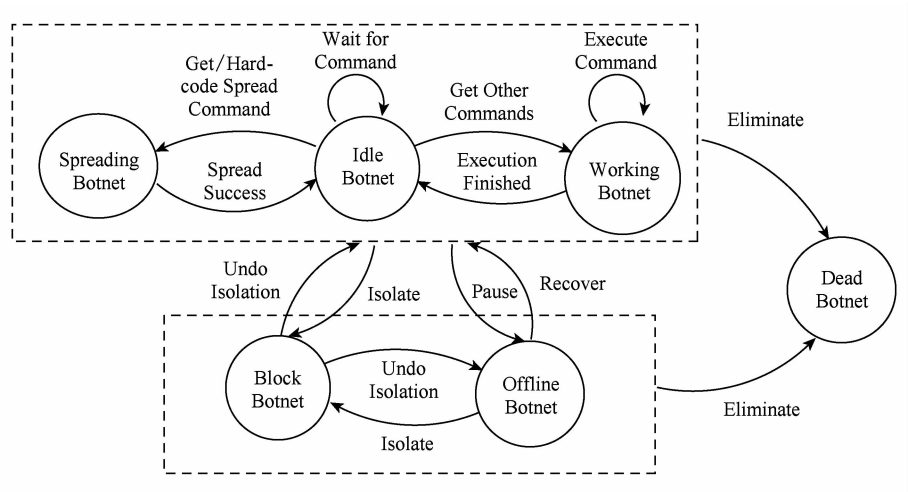


Fig. 3　Status of botnet life-cycle.

图 3　僵尸网络生命周期示意图

1.5　僵尸网络命令控制信道

僵尸网络的本质特性是“可控性”和“协同性”[24],二者实现的关键点在于控制者与肉鸡之间的信息传递和交互,即命令控制信道的实现.命令控制信道决定了僵尸网络的效率和健壮性.一旦其失效,僵尸网络将会瘫痪并降级为离散孤立的、脱离控制源的感染节点集合,威胁性将大大降低.

命令控制信道是攻防双方主控权争夺的关键点.Waledac,MegaD,Mariposa,Zeus Gameover 等名声显赫的僵尸网络受到了来自执法部门、CERT 组织、域名提供商、研究机构的联合反制,致使攻击者失去了控制权,僵尸网络被关闭.对于安全研究人员而言,掌握僵尸网络的拓扑结构和协议特征是开展僵尸网络防御工作的基本前提.

1.5.1　拓扑结构分类

拓扑结构是命令控制信道的基础属性之一,它与僵尸网络的层次划分和通信机制有直接关联[25-27].归纳起来,僵尸网络按拓扑结构可划分为纯中心结构、纯 P2P 结构以及混合结构三大类.

1.5.1.1　纯中心结构

纯中心结构僵尸网络一般采用客户端-服务器(C/S)模式,僵尸主机主动向 C&C 服务器发起请求.如图 4 所示,所有僵尸主机主动访问有限个 C&C 服务器,控制者通过这些服务器向僵尸主机下发控制命令及资源.按照寻址方式,又可将纯中心结构分为静态中心结构和动态中心结构[1].

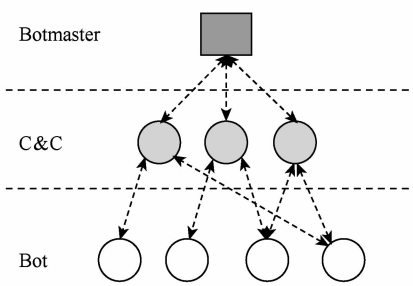


Fig. 4　Pure centralized structure botnets.

图 4　纯中心结构僵尸网络

“静态”指的是 C&C 服务器的域名或 IP 地址是固定的,通常硬编码在僵尸程序体内;“动态”指的是服务器地址并非固定不变,而是需要根据特定算法动态生成[28],该算法事先硬编码在僵尸程序体内,算法的输入是公开可获得的可变内容,比如当前日期、社交网站热点话题等[29].常见的纯中心结构僵尸网络包括 IRC 僵尸网络、HTTP 僵尸网络、

Fast-Flux 僵尸网络以及 Domain-Flux 僵尸网络.

1.5.1.2 纯 P2P 结构

纯中心结构僵尸网络虽具备实现简单、高效、协同性好优势,但其控制流程存在中心节点失效问题(single point of failure),一旦防御人员关闭中心命令控制服务器,僵尸主机将无法继续获取命令,攻击者也将失去对僵尸主机的控制权. 为了提升僵尸网络的健壮性、对抗防御人员的关停,攻击者使用非中心结构的 P2P(peer-to-peer)模式作为其信道拓扑结构,如图 5 所示,网络中每个僵尸主机既充当客户端又充当服务端,通信过程不依赖公网可达服务器资源. 虽然 P2P 僵尸网络命令下发延迟高于中心结构[21],但不依赖脆弱中心节点[30]的特性使其难以被劫持、测量和关闭.

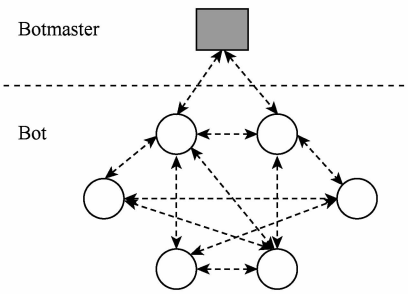


Fig. 5 Pure P2P structure botnets.

图 5 纯 P2P 结构僵尸网络

1.5.1.3 混合结构

混合结构通常指僵尸网络同时具有中心结构和 P2P 结构的部分特性,该类型可进一步划分为 2 个子类:

1) 整体中心结构. 局部 P2P 结构. 如图 6(a)所示,这种混合结构从整体逻辑上看仍属于 C/S 模式的中心结构,但服务节点之间呈现 P2P 结构. 通常公网可达僵尸主机群构成一个动态可扩展的 P2P 网络,形成了一个动态控制服务器池. 该僵尸网络中具有静态 IP、可被外网访问的节点充当 servant bots,此类节点同时扮演服务端和客户端角色,周期性访问其他同类节点,对命令和插件资源进行更新;另一类不具备公网可达属性的节点称为 client bots,由于 NAT 或防火墙等原因,该类节点无法远程被其他节点主动访问,只能向 servant bots 发起连接请求获取命令. 该结构消除了中心节点失效问题,具有较好的可扩展性.

2) 整体 P2P 结构. 该结构是局部中心结构. 如图 6(b)所示,该结构整体上呈现 P2P 结构,在局部实现上呈现 C/S 模式. 其中一部分公网可达的僵尸主机充当服务节点,彼此之间互相连通,同时每个节点独立负责管理一定数量的非公网可达的僵尸主机,这种组网结构有利于实现区域差异化管控,防御者难以探测僵尸网络的所有关键节点和整体规模.

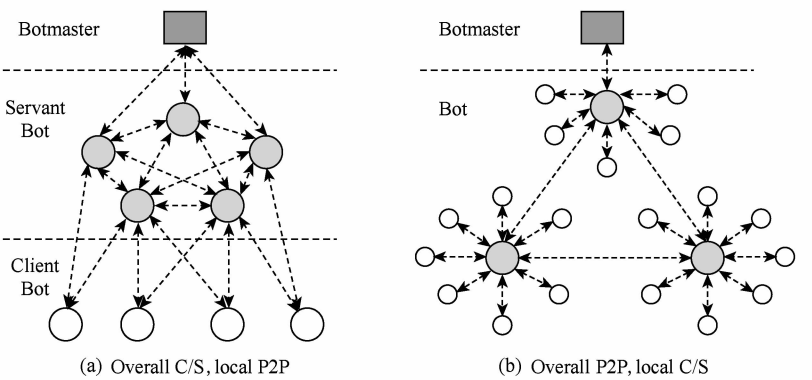


Fig. 6 Hybrid structure botnets.

图 6 混合结构僵尸网络

1.5.2 命令控制协议分类

1.5.2.1 IRC 僵尸网络

基于 IRC 协议的僵尸网络是僵尸网络发展史上的经典,该协议实现较为简单,控制者可借助公共 IRC 聊天室实时下发命令,具备良好的效率.

IRC 僵尸网络命令控制实现过程如下:控制者通常在 IRC 服务器中创建一个聊天室,僵尸程序根据硬编码的地址信息加入该聊天室,静默等待控制者发布命令. 命令的发布主要有 2 种途径:1)TOPIC 方式,僵尸主机登陆聊天室首先会接收到该频道的公告信息,控制者可以将指令发布在公告中,该方式无需控制者实时在线;2)PRIVMSG 方式,在聊天室中,控制者在线通过一对多或一对一的方式向僵尸主机发布指令,该方式最为常见.

1.5.2.2 HTTP 僵尸网络

HTTP 协议具备良好的通用性,能够穿透 IDS

和防火墙,作为 C&C 协议时其流量混杂在大量的正常请求中不易被发现,命令下发延迟低,同时支持对通信内容的加密(HTTPS),因此该协议成为了当前主流的僵尸网络信道协议之一. 命令下发时,攻击者事先将命令内容发布在指定的 Web 网页中,僵尸程序根据硬编码的地址轮询请求获取. 在实现信息回传时,僵尸程序通过 Post 方式将本机信息(bot ID、MAC 地址、操作系统等)或窃取的数据发送给控制者.

传统 HTTP 僵尸网络大多数采用静态寻址方式,C&C 通信易被防御人员识别和阻断. 基于该事实,攻击者们开始尝试使用动态访问机制以增强信道的健壮性,代表性的改进协议包括 Fast-Flux[31] 和 Domain-Flux[29].

1) Fast-Flux 僵尸网络

Fast-Flux 基于多个 IP 和单一域名之间映射关系的快速切换来实现,可以隐藏恶意资源和钓鱼网站的真实 IP. 在僵尸网络中,该协议被控制者用来隐藏 C&C 服务器的真实 IP. 如图 7 所示,僵尸程序解析硬编码的 C&C 域名时,权威 DNS 服务器返回的不是真正的 C&C 服务器(在 Fast-Flux 框架通常称为 mothership[32])IP 地址,而是若干代理节点(称之为 Flux Bot)IP,这些代理节点通常为该僵尸网络中的肉鸡,它们以循环(round-robin)、快速更替的方式充当 C&C 域名的解析地址. 当僵尸主机与 C&C 服务器通信时,Flux Bot 将僵尸主机发来的请求透明转发给 mothership,同时将 mothership 响应信息转发给僵尸主机. 这样,防御人员在追踪僵尸网络通信时,难以发现 mothership 真正的 IP.

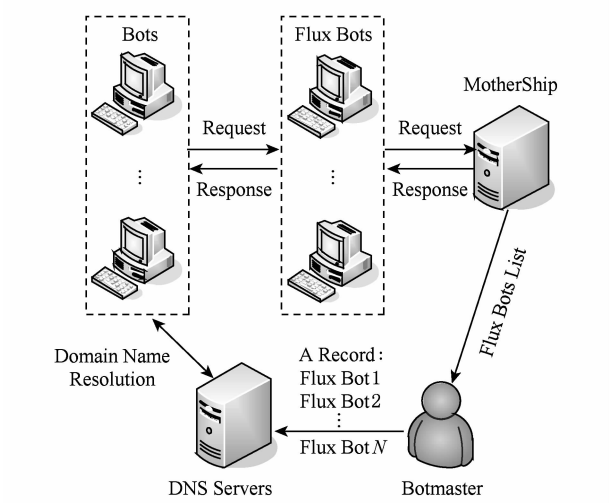


Fig. 7　Implementation of Fast-Flux botnets.

图 7　Fast-Flux 僵尸网络实现原理

该方法使得 C&C 服务器具有大量可更换的 IP 资源,单纯依靠屏蔽 IP 地址的防御手段将无法关闭该僵尸网络. 然而,在 Fast-Flux 实现过程中,其 DNS 请求流量存在短 TTL(time to live)、IP 地理位置分布广、IP 地址跨多个自治系统等特征[33],这些特征可被用来检测和发现 Fast-Flux 僵尸网络的通信行为[34]. 此外,防御人员依旧可以通过屏蔽域名的方法来阻断僵尸网络的 C&C 信道,因此,基于 Fast-Flux 的僵尸网络虽然隐藏了攻击者真实身份,但并未从根本上解决信道脆弱性问题.

2) Domain-Flux 僵尸网络

Domain-Flux 协议的本质是多域名到单个 IP 之间的动态映射. 实现的核心是域名生成算法(domain generation algorithm, DGA),僵尸程序和控制者共享同一套算法,通过相同的输入(日期、话题等)分别计算得到大量相同的域名资源,理论上攻击者只需要将域名资源中任意一个映射到 C&C 服务器 IP 即可保证所有僵尸主机正常获取指令. 由于域名资源数量多且动态变化,防御人员难以完全切断其信道. Torpig,Kraken 和 Conficker 僵尸网络均采用了该协议进行通信.

虽然 Domain-Flux 在一定程度上提高了命令控制信道的健壮性,但其寻址时间开销较长,防御人员可根据大量生成的 NXDomain 报文和域名字符特征 2 个维度对该类型僵尸网络进行检测.

1.5.2.3　P2P 僵尸网络

1) 结构化 P2P. 该类僵尸网络基于结构化 P2P 协议实现,以 2008 年出现的 Storm[35] 为例,该僵尸网络采用基于分布式 Hash 表(distributed hash table, DHT)的 Overnet 协议,在获取命令时僵尸程序以日期和随机数(0～31)作为输入,通过算法生成 32 个不同 Hash key,通过 P2P 网络查询这些 Hash key 值获取控制者指令. 该类型僵尸网络的优点在于信道的构建实现较为便捷、协议稳定可靠,通信流量混杂在合法 P2P 流量中难以被发现.

2) 非结构化 P2P. 僵尸主机间无结构化进行连接,连接方式包含 2 种:①泛洪方式,基于 Random 思想的 Sinit 僵尸网络随机生成 IPV4 地址并逐一对其进行访问验证. 这种协议采用纯 P2P 结构,不存在 bootstrap 阶段且不依赖特定资源节点,十分健壮,然而缺点是节点的连接度很低[12],寻址和通信效率较低,产生的大量扫描流量容易暴露自身;②交换方式,每个僵尸主机维护一份包含节点信息的 peer list,定期随机挑选其中的部分节点进行通信,

获取攻击者指令和更新节点信息,该方式使得僵尸网络具有良好的可扩展性,实现较为灵活.

基于 P2P 协议的僵尸网络虽然在健壮性方面较 HTTP 和 IRC 僵尸网络有所改善,但协议实现过程仍存在 2 个问题:

1) 命令认证的不完备. 由于纯 P2P 僵尸网络中每个节点均可充当服务端,理论上任何人都可以将命令注入到该网络中,这给 P2P 僵尸网络的信息传递带来了隐患. 此外,基于索引模式的 P2P 协议未对索引记录提供者身份进行认证,使得该类 P2P 僵尸网络容易受到索引污染(index poisoning)[36] 和 Sybil 攻击[37-38],命令传递存在被劫持和干扰的可能.

2) 初始化脆弱性. 僵尸主机在初始化过程中需要寻找其他节点并加入该网络,这个过程通常称之为 bootstrap,常见的 bootstrap 方法是僵尸程序访问硬编码的 peer list 或 server cache 中节点,请求加入到僵尸网络中. 由于该过程依赖这些静态寻址资源,一旦失效,新感染的僵尸主机无法加入到网络中接收攻击者指令. 所以,bootstrap 阶段被认为是构建 P2P 僵尸网络的固有脆弱点之一. 例如 Nugache 僵尸网络在该阶段依赖固定的 22 个种子主机地址[39],因此普遍认为其信道具有脆弱性.

2 僵尸网络发展历程

从第 1 个知名的僵尸网络出现至今,僵尸网络的发展历经了十余载,其形态和攻击技术发生了巨大变化,按照时间顺序可将该过程划分为以个人电脑为感染对象的"PC 攻击"(PC attacks) 阶段和以多类型终端为感染目标的"广泛攻击"(extensive attacks) 阶段. 各阶段在终端类型、控制机制、恶意行为等方面存在显著差异.

2.1 PC 攻击阶段

1998—2009 年称为僵尸网络发展史上的"PC 攻击"阶段. 在该时期,僵尸网络以感染 Windows 操作系统的 PC 设备为主,融合了蠕虫传播、rootkit 隐藏、多态变形等多种恶意代码技术[13],在对抗中不断对其信道协议和拓扑结构进行改进,最终发展成为功能多样化、结构复杂化的高级形态.

僵尸网络的起源最早可追溯到 1993 年,当年出现的一款良性 BOT 工具 Eggdrop[40] 能够帮助管理员实现简单的 IRC 网络管理. 受到 Eggdrop 的启发,黑客们开始借鉴其思想,尝试编写恶意的僵尸程序对受害主机实施控制,支配其发动网络攻击. 如图 8 所示,公认的第 1 个知名的恶意僵尸网络 GTBot[41] 诞生于 1998 年,其僵尸程序会在受害主机上隐蔽安装 mIRC 客户端,通过客户端加入 IRC 频道等待控制者下发指令.

在此之后,攻击者们意识到 IRC 协议是一对多进行终端控制的有效方式,包括 PreetyPark, SDbot[42], Agobot[43], Spybot[44], Rbot 在内的 IRC 僵尸网络案例不断出现,其中 Agobot 由于其高度模块化设计、广泛传播、大规模协同攻击特性,使得人们意识到僵尸网络会成为未来互联网安全的重大威胁[21].

虽然 IRC 僵尸网络具有易构建和高效可控的优点,但其流量具有一定特殊性、通信内容为明文传输,导致整个僵尸网络被封锁、检测和监控. 为了解决上述问题,攻击者开始考虑采用 HTTP 和 P2P 协议来进行管控.

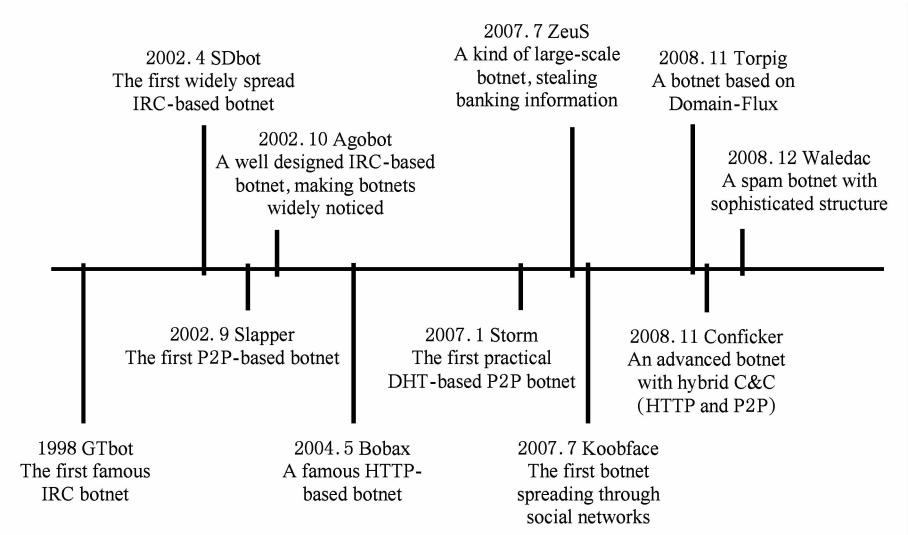


Fig. 8 Botnet cases in PC attacks stage.

图 8 PC 攻击阶段僵尸网络案例

第1个HTTP僵尸网络Bobax[45]出现于2004年,该僵尸网络的主要功能为发送垃圾邮件,通过漏洞利用和邮件方式进行传播;此外,2006年出现的垃圾邮件僵尸网络Rustock和点击欺诈僵尸网络Clickbot以及2007年出现的窃密型僵尸网络ZeuS[46]均采用HTTP作为其命令控制信道协议.

第1个P2P僵尸网络是2002年出现的Slapper,虽然消除了中心节点失效问题,然而通信加密和认证机制的缺失使得信道仍然很脆弱,此后Sinit,Phatbot,Storm的出现证明了P2P僵尸网络具有较好的抗关停能力,研究人员难以对其整体进行测量和监控.

随着攻防博弈的持续升级,攻击者不断改进控制技术以适应于复杂的网络环境,在PC攻击阶段末期,僵尸网络开始呈现协议多样化和结构复杂化的趋势.例如,2008年出现的Conficker僵尸网络同时采用Domain-Flux和Random P2P两种寻址方法,使得防御人员至今难以完全阻断其命令控制信道;同年出现的Waledac[47]综合使用了HTTP,Fast-Flux和P2P协议,具有极好的健壮性和隐秘性.

为了防御未来可能出现的僵尸网络,研究人员尝试提出高级信道模型,对下一代僵尸网络进行预测.Wang等人[48]提出了一种新的混合型P2P僵尸网络命令控制信道,该信道采用层次化结构,bootstrap过程不依赖硬编码的peer list或特定域名资源,消除了单点失效问题.命令传输过程采用非对称密钥加密,难以被防御人员监控和劫持.该方法可以实现负载均衡且具有较好的抗毁能力,因此可管理大规模僵尸网络.其局限在于命令控制信道的构建过程要求传播源必须掌握潜在僵尸主机的IP,因此对钓鱼邮件、P2P文件共享、U盘传播等感染方法无效.

Vogt等人[49]提出了一种混合结构的僵尸网络设计方法,该方法的主要思想是自动把一个大规模僵尸网络划分成多个僵尸子网,僵尸子网之间通过P2P协议连接起来.该方法的优势是彼此独立不易暴露整体规模,可管理大规模僵尸网络而不会出现性能瓶颈.但该结构设计缺乏实践检验,在应对实际复杂的网络环境和防御手段时可能存在不稳定的风险[48].

Hund等人[50]提出了一种难以被追踪和关闭的P2P僵尸网络Rambot,该模型采用基于信誉评分的验证机制(credit-point system)以及工作量证明机制(proof-of-work)等方法判断通信节点身份的真实性,该模型具有一定的智能感知能力,生存性较好.

2.2　广泛攻击阶段

从2009年起至今,僵尸网络呈现出由单一化向多元化发展的趋势,体现在感染对象更加广泛、控制手段更加丰富、应用场景更加精细,其威胁开始逐渐蔓延到了人们日常生活相关的各个领域,该阶段称之为广泛攻击阶段.

如表2所示,广泛攻击阶段出现的新特性有3个方面:1)传统PC僵尸网络与Web 2.0、云计算等新技术广泛融合,出现了更加隐蔽的命令控制技术和特殊形态的僵尸网络;2)伴随着人们日常使用的智能设备和应用日趋丰富,攻击者开始将犯罪目光

Table 2　Comparison Two Stages of PC and Extensive Attacks

表2　PC攻击阶段和广泛攻击阶段对比

Development Phase	Type	Infection Targets	Estimated Size	Topology	Protocols	Malicious Behaviors
PC Attacks	PC botnets	PC	Most hundreds of thousands	Centralized, P2P, Hybrid	IRC, HTTP, P2P, Domain-Flux, Fast-Flux	DDoS, Spamming, Phishing, Online Identity Theft, etc.
Extensive Attacks	PC botnets	PC	Most hundreds of thousands	Most P2P or Hybrid	HTTP, P2P, Domain-Flux, Tor, URL Flux	Bitcoin Theft/Mining, Click Fraud, Ransomware attack, Banking Accounts Theft, etc.
	Emerging botnets	Smartphone, STB, Router, Webcam, POS terminal, Web server, etc.	Most tens of thousands	Centralized	Most IRC and HTTP	DDoS, Spamming, Information Theft, etc.
	Botnets in APT	SCADA, Specific PC	Hundreds to tens of thousands	Centralized or Hybrid	Most HTTP	Destruction and Spy

从传统 PC 转向以智能手机、路由器、机顶盒为代表的多种终端设备;3)僵尸网络构建和命令控制技术在 APT(advanced persistent threat)中得到了广泛应用,成为了攻击链中不可或缺的一环.

2.2.1 PC 僵尸网络新特性

在恶意行为方面,僵尸网络的攻击业务与金融犯罪联系得更加紧密,体现在 3 个方面:1) 金融账户窃取,代表性僵尸网络为 2011 年出现的 Spyeye 和 2014 年发现的 Dridex[51];2)比特币挖掘,2012 年左右活跃的 ZeroAccess 以控制大量受害主机实施点击欺诈和挖掘比特币为目的,每日能获利约 10 万美元[19];3)加密勒索,2013 年以来,伴随着以比特币为代表的匿名支付方式的不断推广,CryptoLocker, CTB-Locker 等加密勒索型僵尸网络案例不断涌现,在该类僵尸网络中僵尸程序通过对受害者文件资源加密实施敲诈,用户需通过比特币交易方式向攻击者支付赎金后方可解密.

在控制机理上,PC 僵尸网络延续了采用复杂的通信手段和拓扑结构对抗关闭的策略. 2011 年出现的 TDL4[52]采用基于 Kad 网络和强加密手段实现通信; ZeuS GameOver[53], ZeroAccess v2[19] 以及 Dride 均采用混合拓扑结构,使得命令控制信道难以被阻断. 与此同时,利用匿名网络构建隐秘的僵尸网络信道也成为了一种新趋势[54-55], Skynet[56] 僵尸网络利用匿名网络 Tor 对命令控制服务器真实地址进行隐藏;Cryptowall 3.0[57] 基于 I2P 匿名网络实现僵尸主机和攻击者之间的通信. 上述案例说明,攻击技术的不断升级给对抗此类高级僵尸网络带来了极大挑战.

以云平台和社交网站为代表的公共服务资源逐渐成为了僵尸网络滋生的沃土. 攻击者们可借助这些公开资源进行传播[20]和命令下发[58-59],防御人员难以发现隐藏在大量合法用户活动中的恶意行为,比如亚马逊 EC2 云被 ZeuS 穿透充当僵尸网络 C&C 服务器[60];以 MAC OS X 为感染目标的 Flashback 僵尸网络[61] 利用 Twitter 构建备用 C&C 信道,一旦主信道失效,僵尸主机将通过搜索动态生成的特定标识寻找 C&C 域名,恢复与控制者间的通信.

此外,僵尸网络行为特性也在逐步与云计算和社交网络相结合,形成基于服务平台的特殊僵尸网络. RSA 2014 大会上,Ragan 和 Salazar[62] 介绍了一种云端僵尸网络的构建方法[63],通过控制海量云计算资源可实现电子货币的挖掘;寄生于社交网站的僵尸网络 SoN(socialbot network)能模仿正常用户完成多种在线社交动作[64],攻击者可通过控制 socialbots 实现谣言散布、广告推送、个人信息收集[65].

在学术界,研究人员也开始研究如何利用其他协议和公开服务构建更为隐蔽的命令控制信道. Xu 等人[66]研究了利用 DNS 协议来构建命令控制信道,该方法无需借助额外的服务器,其下行信道具备良好的隐蔽性;Nappa 等人[67]利用 Skype 协议作为通信载体实现了一种新型僵尸网络,该方法可穿透防火墙和 NAT 设备,其通信流量隐藏在合法 Skype 流量之中,难以被区分和过滤.

Lee 等人提出了一种 Alias-Flux[68] 协议的信道模型,该模型通过恶意利用缩址服务和搜索引擎能实现 bot 对命令控制资源的寻址; Nagaraja 等人[69]提出的信道模型以社交网络作为通信平台,通过图片隐写技术实现命令的传递. Cui 等人[70]提出了一种三信道僵尸网络模型,核心思想是将整个命令控制信道按注册、命令下发、数据回传功能划分为 3 个子信道,分别采用 Domain-Flux, URL-Flux, Cloud-Flux 作为子信道协议,该模型具有较好的生存性和可用性.

2.2.2 新兴僵尸网络崛起

在当今用户安全意识普遍提高、主机防护类软件的普及的背景下,传统 PC 僵尸网络在传播、构建和主机生存性上面临了极大的挑战. 攻击者开始尝试利用非 PC 终端来构建融合网络环境下的僵尸网络,这些设备大多防护手段比较薄弱,容易被渗透和恶意利用. 该类型僵尸网络称之为“新兴僵尸网络”.

2009 年出现的首个手机僵尸网络 Symbian. Yxes 拉开了新兴僵尸网络的序幕,理论上一切连接互联网且具有运算能力的终端都可成为潜在的僵尸主机. 路由器、PoS 机、机顶盒、网络摄像头、智能家居、Web 服务器等设备[71-73]成为了首选感染目标. 攻击者在利用这些设备发起传统网络攻击的同时,还可对用户信息进行窃取. 2010 年出现的首个针对 Android 系统的手机僵尸网络 Geinimi[74] 可实现 IMEI、地理位置、短信、通信录等信息的窃取,同时还能发送垃圾短信和安装恶意软件;2012 年首个 POS 机僵尸网络 Dexter 通过内存读取技术大量窃取用户的支付卡数据;2015 年出现的 Moose[75] 可通过路由器流量监听窃取用户社交网站账号,通过

“卖粉”形式盈利.

不同于主流 PC 僵尸网络采用的邮件附件、网页挂马、软件捆绑和 PPI 的传播方法,绝大多数新兴僵尸网络传播以口令暴力猜解和固件漏洞利用的方法为主,实现成本较低且无需用户配合,攻击者可轻松实现大规模自动化的渗透. 2012 年出现的 Carna 僵尸网络通过扫描弱口令全球范围内感染了约 42 万台嵌入式设备,获取了约 9TB 通信日志[76]. 此外,部分新兴僵尸网络具备跨平台特性,感染终端范围更加广泛. 例如 Darlloz 僵尸网络可同时感染 x86,ARM,MIPS 以及 PowerPC 在内的多种架构设备[77].

在运行终端和平台趋于丰富的同时,新兴僵尸网络的通信协议通常采用 HTTP 和 IRC 协议,寻址策略通常采用硬编码地址方式,通信内容通常采用简单加密和混淆来躲避检测,可满足实时控制需求,该种模式在具备易用性和高效性的同时其信道健壮性较差. 这表明新兴僵尸网络的命令控制方式较为简单和脆弱,同当今复杂的高级 PC 僵尸网络相比仍有一定的差距.

在众多新兴僵尸网络中,智能手机以其用户数量大、信息资源丰富、计算能力强、软件种类多的特点,成为了研究人员的主要研究方向,该类僵尸网络也被称为移动僵尸网络. 在预测工作中,研究人员需考虑手机应用场景下的特有限制条件,包括固定 IP 资源缺乏、电量消耗以及用户资费敏感等问题. 因此,当前移动僵尸网络的预测主要围绕隐蔽可行的信道协议设计为主.

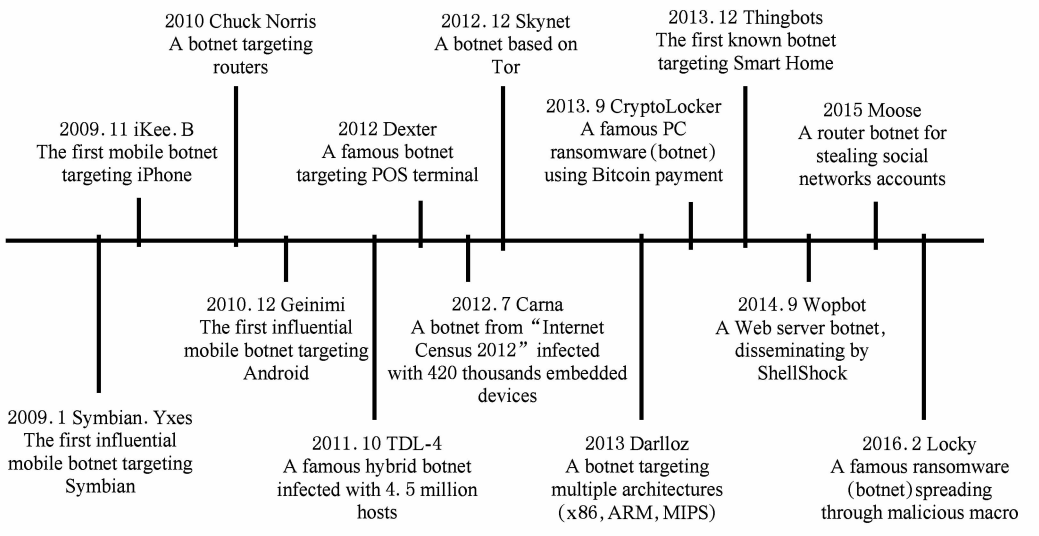


Fig. 9　Botnet cases in Extensive Attacks stage.

图 9　广泛攻击阶段僵尸网络案例

早期移动僵尸网络的信息传递大多采用 SMS 实现. Mulliner 等人[78]提出了一种 SMS-HTTP 混合结构的命令控制信道. 主要思路是将控制命令分发分为 2 个步骤:1)将加密签名过的控制命令发布到网站上;2)通过 SMS 将控制命令 URL 推送给僵尸程序. Zeng 等人[79]提出了一种利用 SMS 构建的 P2P 命令控制信道,SMS 作为命令控制信道具有时效性强、健壮性好、离线用户(如关机、不在服务区等)可延迟接收等优点,但利用 SMS 建立和维持一个可连通的僵尸网络拓扑关系,需要发送和接受极大数量的 SMS,造成用户端资费和信息的明显异常.

Singh 等人[80]提出并评估了使用蓝牙作为命令控制信道的可行性:其优点在于健壮性好,不会产生额外的资费开销;缺点是时效性差,蓝牙传输的距离限制造成了通信效率的低下,在实际应用中存在问题.

Cui 等人[16]提出了一种基于 URL-Flux 动态中心结构的移动僵尸网络 Andbot,该方法利用博客和微博作为其资源发布平台,通过 UGA 算法 bot 可以动态从大量生成的 URL 中去寻找命令资源. 该方法具有良好的隐蔽性和韧性,运用在智能手机场景中能满足低能耗和低资费需求.

Zhao 等人[81]提出了一种基于 Google 云推送服务(cloud to device message, C2DM)的移动僵尸网络. 僵尸主机与合法云信息服务器(C2DM server)进行交互,不访问可疑域名或 IP 资源,不依赖资费敏感的 SMS,同时不会遗漏离线状态下发送的命令,其通信流量较传统 HTTP 和 IRC 移动僵尸网络更小,

该方法较之前的研究具有更好的隐蔽性和可控性.

2.2.3 APT 中僵尸网络

近年来,以“震网”[82]、“火焰”[83]、Duqu[84]、“红色十月”[85]、DarkHotel[86]、Turla[22]为代表的 APT 攻击不断出现,针对各国政府、军队、能源、工业、科研机构等重要目标展开网络间谍和破坏活动,严重威胁着国家的政治、经济和军事安全.以卡巴斯基、赛门铁克为代表的安全厂商对有关案例进行了深入的跟踪分析,揭示了背后的攻击流程和常用手法.

在完整攻击链中,攻击者通常在感染立足点后进行内部横向平移,构建小型僵尸网络.感染主机通过代理[87]或隐蔽直连方式同外界建立通信,获取攻击者指令或实现窃密回传[88],此类方法与传统僵尸网络的控制方法极其相似.在 Duqu 2.0 中[89],感染主机将信息隐藏在 GIF 和 JPEG 图片中,通过感染的网关和防火墙作为中转发送给外部攻击者.DUKES 黑客组织在 APT 攻击中利用日期算法生成用户名,通过 Twitter 和 Github 平台查找该用户信息获取指令[90].

在部分 APT 攻击中,攻击者直接使用公开的僵尸网络套件实施攻击.绰号“沙虫”(Sandworm)的黑客组织[91]于 2014 年和 2015 年 12 月利用开源的 BlackEnergy 攻击套件分别对欧美 SCADA 工控系统和乌克兰电网系统发动攻击.

虽然 APT 攻击与普通僵尸网络在命令控制机制上具有高度相似性,但二者在规模和信道属性上存在一定差异:在规模上,传统僵尸网络侧重大规模、无差别的感染和控制,而 APT 强调对少数特定目标进行感染和控制;在信道属性上,僵尸网络强调对大规模肉鸡的管控,要求其控制信道具有良好的健壮性,而 APT 攻击强调对少数目标的隐蔽和持续性控制,其 C&C 信道部分侧重于易用和隐蔽性,不考虑依托复杂的信道结构和协议来对抗关闭.此外,APT 攻击中的通信实现更趋于精细化和复杂化,2015 年 12 月,卡巴斯基披露的间谍组织 Turla[92]在攻击过程中利用劫持卫星通信的方式实现信息传递,如图 10 所示,防御人员难以对攻击者进行溯源,该种技术是普通僵尸网络所不具备的.

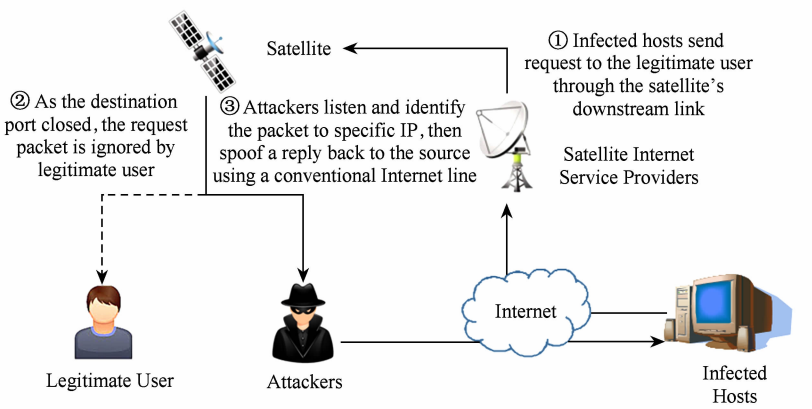


Fig. 10 Anonymous C&C communication by hijacking satellite link.

图 10 通过卫星链路劫持实现匿名 C&C 通信

3 僵尸网络对抗

准确发现僵尸网络的存在,进一步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.具体地,该部分工作可分为检测和遏制 2 个部分:检测工作旨在发现僵尸主机、通信活动以及命令控制服务器;而遏制工作则注重利用主动清除的手段将僵尸网络危害降到最低.

3.1 僵尸网络检测

从技术实现角度出发,已知检测方法通常可划分为基于蜜罐分析、基于通信特征码、基于异常、基于日志 4 类.

3.1.1 基于蜜罐分析检测

基于蜜罐分析检测方法首先通过蜜罐诱捕的方法获取大量恶意代码样本,在可控环境中进行监控分析,发现僵尸程序及其恶意行为.代表性的蜜罐包括 Argos, Nepen-thes, Sebek 等.该方法可发现未知僵尸网络的行为特征,有助于进一步了解僵尸网络通信机理及潜在脆弱点;缺点是难以发现通过社工方式传播的僵尸网络,难以全面发现其他已感染节点,由于缺乏用户操作,容易被具有反蜜罐功能的僵尸

程序所识别[93].

3.1.2　基于通信特征码检测

基于通信特征码检测的方法是普遍采用的防御方法,通过事先配置特征匹配规则,诸如 Snort 等传统入侵检测系统可快速、准确发现僵尸网络活动.该方法适用于具有明确特征的僵尸网络,缺点是无法检测特征未知的僵尸网络,需要持续维护和更新特征码知识库,提高了检测成本.

3.1.3　基于异常检测

基于异常检测的方法主要围绕僵尸网络引发的异常进行检测,具体又可分为主机层异常检测和网络层异常检测.

主机层异常检测通过监控终端行为发现异常,监控内容包括进程、文件、注册表、网络连接等行为.Stinson 等人[94]假定僵尸程序接收远程控制命令后其行为与正常进程行为具有差异性,基于该假设提出的 BotSwat 能通过监控系统调用及其执行参数来识别僵尸程序,该方法具有较高的准确率且与 C&C 协议无关.

网络层异常检测假定僵尸程序与控制服务器之间的通信模式较正常用户通信具有显著差异,可通过流量分析来发现僵尸网络的踪迹,常见的异常特征包括高网络延迟、高流量、非常规端口流量等[14].Karasaridis 等人[95]提出了一种基于传输层流数据的检测方法,该方法能检测加密的僵尸网络通信,同时可以帮助识别僵尸网络规模和特征;Manos Antonakakis 等人[8]根据 Domain-Flux 僵尸网络产生大量 NXDomain 流量的特点提出了一种检测方法,可识别僵尸网络 DGA 类型;Gu 等人[24]提出的 BotMiner 首先对数据流按目的地址和端口进行划分,经过流量属性聚类和主机异常行为关联分析后检测出可疑的僵尸网络通信,该方法同样具有协议无关性;Leyla 等人[96]提出一种面向 NetFlow 数据、动态选取特征的高速检测系统 DISCLOSURE,该系统克服了检测特征固定的脆弱性,在不同应用场景可自适应平衡误报率和漏报率,每日可检测十亿级规模的流数据.

3.1.4　基于日志检测

基于日志检测的方法与基于异常检测的方法比较相似,但数据源大多来自 DNS、邮件等日志记录.研究人员通过分析日志中的异常来识别可能的僵尸网络行为.Choi 等人[97]通过监测 DNS 查询流量的群体活动特性来发现僵尸网络;基于垃圾邮件内容相似性,Zhuang 等人[98]对垃圾邮件进行分组,根据不同分组中发送人 IP 信息进行进一步分析,识别不同类型的僵尸网络;假定攻击者可能使用“同一 IP 地址短时间内注册大量邮件账户”以及“同一邮件账号短时间跨 AS 域发送大量垃圾邮件”,Zhao 等人提出了一种基于图论的关联分析系统 BotGraph[99],该系统可通过分析邮件服务器中账号激活及登录日志来发现垃圾邮件型僵尸网络.

3.2　僵尸网络遏制

通过检测分析掌握了僵尸网络相关信息后,研究人员需要联合有关组织和部门、运用技术手段对僵尸网络传播和通信进行对抗,该种行为通常称为遏制(mitigation),如图 11 所示,常见手段包括终端清除、命令控制过程对抗以及命令控制服务器打击三大类.

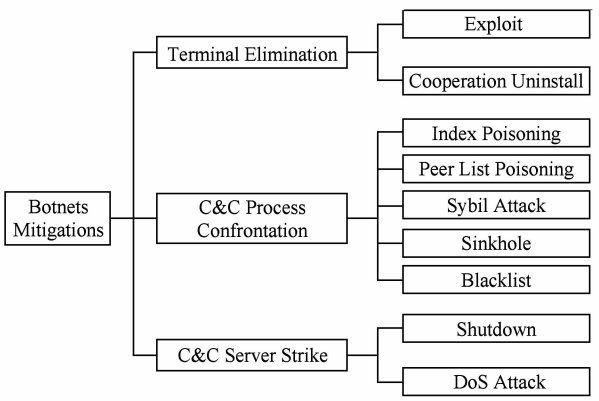


Fig. 11　Classification of botnets mitigations.

图 11　僵尸网络遏制方法分类

3.2.1　终端清除

终端清除主要指清除已感染终端的僵尸程序.防御人员可以通过挖掘并利用僵尸程序自身漏洞来实现清除[11],而更加通用的做法是联合大型反病毒公司、系统厂商以及互联网服务提供商(ISP)对感染终端进行定位,帮助用户进行清理.2014 年初,微软安全部门远程帮助用户移除 Sefnit 僵尸程序以及包含漏洞的 Tor 客户端,使得 Tor 网络中用户数量下降了约 200 万[100];Hadi 等人[9]利用 sinkhole 日志数据对过去 6 年 Conficker 终端清理效果进行了评估,证明以国家为单位的僵尸网络打击方案收效甚微,呼吁各国 ISP 应当承担更多监控和清理责任.

3.2.2　命令控制过程对抗

僵尸网络通信协议在实现过程中可能存在某些脆弱点,比如单点失效问题、控制者身份未识别、命令时效性未校验等.防御人员利用该类缺陷不仅可干扰和阻断僵尸网络的正常命令下发,甚至可以接管其控制权,该类方法统称为命令控制过程对抗技术.

对于 P2P 僵尸网络而言,常用对抗手段包括索引污染、Sybil 攻击以及 peer list 污染 3 种. 例如,DHT 思想的 P2P 僵尸网络易受到索引污染和 Sybil 攻击,Davis 等人[38]利用 Sybil 攻击对 Storm 实施了拒绝服务攻击;而采用 peer list 交换路由的 P2P 僵尸网络易遭受 peer list 污染,Waledac 僵尸网络在其自定义的 P2P 协议中,peer 之间交换路由没有认证机制,遭到了微软连同学术研究机构对其 Repeater 节点 peer 地址表的污染,导致其命令控制信道失效.

对于中心结构僵尸网络,由于其中心节点失效缺陷,防御人员不仅可以通过 IP、域名、URL 黑名单的方法阻断僵尸网络通信,还可基于 sinkhole 的思想将 C&C 域名指向自主可控的资源,实现僵尸网络的测量或劫持. 利用僵尸程序对 C&C 服务器身份未进行鉴别的缺陷,Stone-Gross 等人[28]和 Amini 等人[101]通过 sinkhole 的方式成功劫持了基于 Domain-Flux 协议的 Torpig 和 Kraken 僵尸网络.

3.2.3 命令控制服务器打击

直接打击 C&C 服务器也是常见的对抗手段之一,具体方法包括:1)物理关闭,联合有关服务提供商直接关停 C&C 服务器,但攻击者可通过重新搭建来恢复控制;2)DoS,防御人员可以对僵尸网络的中心服务器或关键节点(比如 Fast-Flux 中权威域名服务器)进行拒绝服务攻击[102],延缓僵尸主机正常获取指令时间,降低其整体可用性.

4 研究现状及思考

4.1 已有研究存在的问题

在信道预测方向上,已有工作集中围绕构建隐蔽或健壮的命令控制信道为主,大多存在实现过程复杂、可用性差的特点,未涉及智能感知和多终端跨平台管控,难以真正代表未来僵尸网络的发展趋势.

在僵尸网络检测方向上,以网络通信流为对象、基于机器学习算法实现的检测方法是主流研究方向,但已有成果大多存在检测耗时较长、特征依赖的问题,难以兼顾准确性和性能需求.

在僵尸网络对抗上,目前存在法律监管、各国间信息共享和机构间协调等非技术难题,需要全球范围内有关机构和组织进一步重视僵尸网络问题,形成高效、全面、长期的合作应对机制.

4.2 未来研究方向

综合上述讨论,结合当前僵尸网络发展态势,未来僵尸网络领域的研究重点包括:1)关注海量异构化脆弱终端的发现和渗透技术,研究相应的检测和防御方法;2)基于终端数据的回收分析,研究智能感知型僵尸网络管控技术;3)研究僵尸网络演化与地下黑市中动态的关联性,从供应链的角度提出防治僵尸网络的方法.

5 总 结

作为传统恶意代码的演化形态,僵尸网络为控制者提供了一种灵活高效的命令控制机制,是实现 DDoS、垃圾邮件、信息窃取、点击欺诈、恶意软件分发的理想平台. 随着融合网络时代的到来,僵尸网络在感染对象、管控技术、恶意行为方面有了新的变化,这将给未来互联网安全造成更大的威胁.

本文在全面介绍僵尸网络机理特性的基础上,按时间顺序将僵尸网络发展史划分为 PC 攻击和广泛攻击 2 阶段,详细介绍各阶段特点和典型案例,总结僵尸网络发展态势. 对已有检测和遏制手段进行了归纳分析,小结当今僵尸网络研究存在的不足,预测未来可能的研究热点.

考虑到当前互联网技术更新以及僵尸网络发展呈现的新趋势,安全领域研究人员必须加强对僵尸网络的研究,协同各安全厂商和政府监管部门共同应对日趋严峻的威胁.

参 考 文 献

[1] Fang Binxing, Cui Xiang, Wang Wei. Survey of botnets [J]. Journal of Computer Research and Development, 2011, 48(8): 1315-1331 (in Chinese)
(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)

[2] McAfee Communities. McAfee Labs Threat Advisory CTB-Locker. (2015-02-09)[2016-06-14]. https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25696/en_US/McAfee_Labs_Threat_Advisory-CTB-Locker.pdf

[3] 国家应急响应中心. CNCERT 互联网安全威胁报告-2016 年 3 月[EB/OL]. (2016-03-17)[2016-06-14]. http://www.cert.org.cn/publish/main/upload/File/2016monthly03.pdf

[4] Symantec. Internet Security Threat Report 2014 [EB/OL]. 2014[2016-06-14]. https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[5] Kaspersky Lab. Statistics on botnet-assisted DDoS attacks in Q1 2015 [EB/OL]. 2015[2016-06-14]. https://securelist.com/blog/research/70071/statistics-on-botnet-assisted-ddos-attacks-in-q1-2015

[6] Symantec. Internet Security Threat Report [EB/OL]. 2016 [2016-06-14]. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[7] Nadji Y, Antonakakis M, Perdisci R, et al. Beheading hydras: Performing effective botnet takedowns [C] //Proc of the 2013 ACM SIGSAC Conf on Computer & Communications Security. New York: ACM, 2013: 121-132

[8] Antonakakis M, Perdisci R, Nadji Y, et al. From throw-away traffic to bots: Detecting the rise of DGA-based malware [C] //Proc of the 21st USENIX Security Symp (USENIX Security 12). Berkeley, CA: USENIX Association, 2012: 491-506

[9] Asghari H, Ciere M, Van Eeten M J G. Post-mortem of a zombie: Conficker cleanup after six years [C] //Proc of the 24th USENIX Security Symposium (USENIX Security 15). Berkeley, CA: USENIX Association, 2015

[10] Xie Y, Yu F, Achan K, et al. Spamming botnets: Signatures and characteristics [J]. ACM SIGCOMM Computer Communication Review, 2008, 38(4): 171-182

[11] Dittrich D. So you want to take over a Botnet [C] //Proc of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats. Berkeley, CA: USENIX Association, 2012

[12] Zhuge Jianwei, Han Xinhui, Zhou Yonglin, et al. Research and development of botnets [J]. Journal of Software, 2008, 19(3): 702-715 (in Chinese)
(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)

[13] Jiang Jian, Zhuge Jianwei, Duan Haixin, et al. Research on botnet mechanisms and defenses [J]. Journal of Software, 2012, 23(1): 82-96 (in Chinese)
(江健, 诸葛建伟, 段海新, 等. 僵尸网络机理与防御技术[J]. 软件学报, 2012, 23(1): 82-96)

[14] Silva S S C, Silva R M P, Pinto R C G, et al. Botnets: A survey [J]. Computer Networks, 2013, 57(2): 378-403

[15] Puri R. Bots & botnet: An overview [R/OL]. Los Angeles: SANS Institute, 2003 [2016-06-01]. https://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299

[16] Cui Xiang, Fang Binxing, Yin Lihua, et al. Andbot: Towards advanced mobile botnets [C] //Proc of the 4th USENIX Conf on Large-Scale Exploits and Emergent Threats. Berkeley, CA: USENIX Association, 2011

[17] BrianKrebs. Botcoin: Bitcoin Mining by Botnet [EB/OL]. (2013-07-18) [2016-06-14]. http://krebsonsecurity.com/2013/07/botcoin-bitcoin-mining-by-botnet

[18] Goebel J, Holz T. Rishi: Identify bot contaminated hosts by IRC nickname evaluation [C] //Proc of the 1st Conf on Hot Topics in Understanding Botnets. Berkeley, CA: USENIX Association, 2007

[19] Wyke J. The ZeroAccess botnet-Mining and fraud for massive financial gain [R/OL]. Oxford, UK: SophosLabs, 2012 [2016-06-01]. https://www.sophos.com/en-us/threat-center/technical-papers/zeroaccess-botnet.aspx

[20] Baltazar J, Costoya J, Flores R. The real face of koobface: The largest Web 2.0 botnet explained [J]. Trend Micro Research, 2009, 5(9): 10-28

[21] Grizzard B, Sharma V, Nunnery C, et al. Peer-to-peer botnets: Overview and case study [C] //Proc of the 1st Conf on Workshop on Hot Topics in Understanding Botnets. Berkeley, CA: USENIX Association, 2007

[22] Gu L. Prototype Nation: The Chinese Cybercriminal Underground in 2015 [EB/OL]. (2015-11-23)[2016-06-14]. https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-prototype-nation.pdf

[23] Sood A K, Enbody R J, Bansal R. Dissecting SpyEye-Understanding the design of third generation botnets [J]. Computer Networks, 2013, 57(2): 436-450

[24] Gu G, Perdisci R, Zhang J, et al. BotMiner: Clustering analysis of network traffic for protocol-and structure-independent botnet detection [C] //Proc of USENIX Security Symp. Berkeley, CA: USENIX Association, 2008: 139-154

[25] Dagon D, Gu G, Lee C P, et al. A taxonomy of botnet structures [C] //Proc of the 23rd Annual Computer Security Applications Conf (ACSAC 2007). Piscataway, NJ: IEEE, 2007: 325-339

[26] Cooke E, Jahanian F, McPherson D. The zombie roundup: Understanding, detecting, and disrupting botnets [C] //Proc of the USENIX SRUTI Workshop 2005. Berkeley, CA: USENIX Association, 2005

[27] Liu L, Chen S, Yan G, et al. Bottracer: Execution-based bot-like malware detection [G] //Information Security. Berlin: Springer, 2008: 97-113

[28] Stone-Gross B, Cova M, Cavallaro L, et al. Your botnet is my botnet: Analysis of a botnet takeover [C] //Proc of the 16th ACM Conf on Computer and Communications Security. New York: ACM, 2009: 635-647

[29] Zhang L, Yu S, Wu D, et al. A survey on latest botnet attack and defense [C] //Proc of the 10th IEEE Int Conf on Trust, Security and Privacy in Computing and Communications. Piscataway, NJ: IEEE, 2011: 53-60

[30] Feily M, Shahrestani A, Ramadass S. A survey of botnet and botnet detection [C] //Proc of the 3rd Int Conf on Emerging Security Information, Systems and Technologies. Piscataway, NJ: IEEE, 2009: 268-273

[31] Riden J. Know your Enemy: Fast-Flux service networks [R/OL]. Ann Arbor, MI: The Honeynet Project, 2008 [2016-06-01]. http://www.honeynet.org/book/export/html/130

[32] Nazario J, Holz T. As the net churns: Fast-Flux botnet observations [C] //Proc of the 3rd Int Conf on Malicious and Unwanted Software. Piscataway, NJ: IEEE, 2008: 24-31

[33] Mahmoud M, Nir M, Matrawy A. A survey on botnet architectures, detection and defences [J]. International Journal of Network Security, 2015, 17(3): 272-289

[34] Holz T, Gorecki C, Rieck K, et al. Measuring and detecting Fast-Flux service networks [C/OL] //Proc of the 2008 Network and Distributed System Security Conf. 2008. [2016-06-11]. http://ei. rub. de/media/emma/veroeffentlichungen/2012/08/07/FastFlux-NDSS08. pdf

[35] Holz T, Steiner M, Dahl F, et al. Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm [C] //Proc of the 1st USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET'08). Berkeley, CA: USENIX Association, 2008

[36] Liang J, Naoumov N, Ross K W. The index poisoning attack in P2P file sharing systems [C] //Proc of the IEEE INFOCOM 2006. Piscataway, NJ: IEEE, 2006: 1-12

[37] Wang P, Wu L, Aslam B, et al. A systematic study on peer-to-peer botnets [C] //Proc of the 18th Int Conf on Computer Communications and Networks (ICCCN 2009). Piscataway, NJ: IEEE, 2009: 1-8

[38] Davis C R, Fernandez J M, Neville S, et al. Sybil attacks as a mitigation strategy against the storm botnet [C] //Proc of the 3rd Int Conf on Malicious and Unwanted Software (MALWARE 2008). Piscataway, NJ: IEEE, 2008: 32-40

[39] Dittrich D, Dietrich S. P2P as botnet command and control: A deeper insight [C] //Proc of the 3rd Int Conf on Malicious and Unwanted Software (MALWARE 2008). Piscataway, NJ: IEEE, 2008: 41-48

[40] Pointer R. EggHeads. org-eggdrop development [EB/OL]. 1993 [2016-06-14]. http://dumbledore. hubpages. com

[41] Macesanu G, Codas T T, Suliman C, et al. Development of GTBoT, a high performance and modular indoor robot [C] // Proc of the 2010 IEEE Int Conf on Automation Quality and Testing Robotics (AQTR). Piscataway, NJ: IEEE, 2010

[42] Micro T. Worm SDBot [EB/OL]. 2003 [2016-06-14]. http://about-threats. trendmicro. com/ArchiveMalware. aspx?language=us&-name=WORMSDBOT. AZ

[43] Micro T. Worm AgoBot [EB/OL]. 2004 [2016-06-14]. http://about-threats. trendmicro. com/ArchiveMalware. aspx?language=us&-name=WORMAGOBOT. XE

[44] Symantec. Spybot worm [EB/OL]. 2003 [2016-06-14]. http://www. symantec. com/securityresponse/writeup. jsp?docid=2003-053013-5943-99

[45] Ramachandran A, Feamster N. Understanding the network-level behavior of spammers [C] //Proc of the 2006 Conf on Applications, Technologies, Architectures and Protocols for Computer Communications. New York: ACM, 2006: 291-302

[46] Binsalleeh H, Ormerod T, Boukhtouta A, et al. On the analysis of the zeus botnet crimeware toolkit [C] //Proc of the 8th Annual Int Conf on Privacy Security and Trust (PST). Piscataway, NJ: IEEE, 2010: 31-38

[47] Stock B, Engelberth M, Freiling F C, et al. Walowdac analysis of a peer-to-peer botnet [C] //Proc of the 2009 European Conf on Computer Network Defense. Los Alamitos, CA: IEEE Computer Society, 2009: 13-20

[48] Wang P, Sparks S, Zou C C. An advanced hybrid peer-to-peer botnet [J]. IEEE Trans on Dependable and Secure Computing, 2010, 7(2): 113-127

[49] Vogt R, Aycock J, Jacobson M J. Army of botnets [C/OL] //Proc of the 2008 Network and Distributed System Security Conf. 2007 [2016-06-11]. http://www. internetsociety. org/sites/default/files/Army% 20of% 20Botnets% 20 (Ryan% 20Vogt). pdf

[50] Hund R, Hamann M, Holz T. Towards next-generation botnets [C] //Proc of the European Conf on Computer Network Defense (EC2ND 2008). Piscataway, NJ: IEEE, 2008: 33-40

[51] Blueliv. Chasing cybercrime: Network insights of dyre and dridex trojan bankers [EB/OL]. (2015-04-22) [2016-06-14]. https://www. blueliv. com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bankers. pdf

[52] Rodionov E, Matrosov A. The evolution of tdl: Conquering x64 [EB/OL]. 2011 [2016-06-11]. http://www. welivesecurity. com/media_files/white-papers/The_Evolution_of_TDL. pdf

[53] abuse. ch. Zeus gets more sophisticated using P2P techniques [EB/OL]. (2011-10-10) [2016-06-14]. http://www. abuse. ch/?p=3499

[54] Casenove M, Miraglia A. Botnet over Tor: The illusion of hiding [C] //Proc of the 6th Int Conf On Cyber Conflict (CyCon 2014). Piscataway, NJ: IEEE, 2014: 273-282

[55] Klijnsma Y. Large botnet cause of recent Tor network overload [EB/OL]. (2013-09-05) [2016-06-14]. https://blog. fox-it. com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload

[56] Nex. Skynet, a Tor-powered botnet straight from Reddit [EB/OL]. (2012-12-03) [2016-06-14]. https://community. rapid7. com/community/infosec/blog/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit

[57] Dontnc M. Guess who's back again? Cryptowall 3. 0 [EB/OL]. (2015-01-13) [2016-06-14]. http://malware. dontneedcoffee. com/2015/01/guess-whos-back-again-cryptowall-30. html

[58] Kartaltepe E J, Morales J A, Xu S, et al. Social network-based botnet command-and-control: Emerging threats and countermeasures [C] //Proc of the Applied Cryptography and Network Security. Berlin: Springer, 2010: 511-528

[59] Boshmaf Y, Muslukhov I, Beznosov K, et al. Design and analysis of a social botnet [J]. Computer Networks, 2013, 57(2): 556-578

[60] Goodin D. Zeus bot found using amazon's ec2 as c and c server [EB/OL]. (2009-12-09) [2016-06-14]. http://www. theregister. co. uk/2009/12/09/amazon ec2 bot control channel

[61] Prince B. Flashback botnet updated to include twitter as C&C [EB/OL]. (2012-04-30) [2016-06-14]. http://www. securityweek. com/flashback-botnet-updated-include-twitter-cc

[62] Ragan R, Salazar O. Cloudbots: Harvesting crypto coins like a botnet farmer [EB/OL]. 2014[2016-06-14]. https://www.syscan360.org/slides/2014_EN_CloudBots_RobRaganOscarSalazar.pdf

[63] Higgins K J. Smartphone weather app builds a mobile botnet [EB/OL]. (2010-03-05) [2016-06-14]. http://www.darkreading.com/risk/smartphone-weather-app-builds-a-mobile-botnet/d/d-id/1133138

[64] Boshmaf Y, Muslukhov I, Beznosov K, et al. The socialbot network: When bots socialize for fame and money [C] //Proc of the 27th Annual Computer Security Applications Conf. New York: ACM, 2011: 93-102

[65] Boshmaf Y, Muslukhov I, Beznosov K, et al. Key challenges in defending against malicious socialbots [C] //Proc of the 5th USENIX Conf on Large-Scale Exploits and Emergent Threats. Berkeley, CA: USENIX Association, 2012: 12-12

[66] Xu K, Butler P, Saha S, et al. DNS for massive-scale command and control [J]. IEEE Trans on Dependable and Secure Computing, 2013, 10(3): 143-153

[67] Nappa A, Fattori A, Balduzzi M, et al. Take a deep breath: A stealthy, resilient and cost-effective botnet using skype [C] //Proc of the Int Conf on Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin: Springer, 2010: 81-100

[68] Lee S, Kim J. Fluxing botnet command and control channels with URL shortening services [J]. Computer Communications, 2013, 36(3): 320-332

[69] Nagaraja S, Houmansadr A, Piyawongwisal P, et al. Stegobot: A covert social network botnet [C] //Proc of the 13th Int Conf on Information Hiding. Berlin: Springer, 2011: 299-313

[70] Cui Xiang, Fang Binxing, Shi Jinqiao, et al. Botnet triple-channel model: Towards resilient and efficient bidirectional communication botnets [C] //Proc of the 9th Int Conf on Security and Privacy in Communication Networks. Berlin: Springer, 2013: 53-68

[71] Proofpoint. Proofpoint uncovers Internet of things (IoT) cyberattack [EB/OL]. (2014-01-16) [2016-06-14]. https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack

[72] Rights RF. Analyzing a backdoor/bot for the MIPS platform [EB/OL]. 2015 [2016-06-14]. http://www.sans.org/reading-room/whitepapers/malicious/analyzing-backdoor-bot-mips-platform-35902

[73] Saarinen J. First Shellshock botnet attacks Akamai, US DoD networks [EB/OL]. (2014-09-26) [2016-06-14]. http://www.itnews.com.au/news/first-shellshock-botnet-attacks-akamai-us-dod-networks-396197

[74] Wyatt T. Security alert: Geinimi, sophisticated new Android Trojan found in wild [EB/OL]. (2010-09-29) [2016-06-14]. https://blog.lookout.com/blog/2010/12/29/geinimi_trojan

[75] Bilodeau O, Dupuy T. Dissecting Linux/Moose [EB/OL]. 2015 [2016-06-14]. http://www.welivesecurity.com/wp-content/uploads/2015/05/Dissecting-LinuxMoose.pdf

[76] Botnet C. Internet census 2012 [EB/OL]. 2012 [2016-06-14]. http://internetcensus2012.bitbucket.org/paper.html

[77] Ullrich J. More Device Malware: This is why your DVR attacked my Synology Disk Station (and now with Bitcoin Miner!) [EB/OL]. 2014[2016-06-14]. https://isc.sans.edu/forums/diary/More+Device+Malware+This+is+why+your+DVR+attacked+my+Synology+Disk+Station+and+now+with+Bitcoin+Miner/17879

[78] Mulliner C, SeifertIn J.P. Rise of the iBots: Owning a telco network [C] //Proc of the 5th IEEE Int Conf on Malicious and Unwanted Software (Malware) Nancy. Piscataway, NJ: IEEE, 2010: 71-80

[79] Zeng Y, Shin K G, Hu X. Design of SMS commanded-and-controlled and P2P-structured mobile botnets [C] //Proc of the 5th ACM Conf on Security and Privacy in Wireless and Mobile Networks. New York: ACM, 2012: 137-148

[80] Singh K, Sangal S, Jain N, et al. Evaluating bluetooth as a medium for botnet command and control [C] //Proc of the Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin: Springer, 2010: 61-80

[81] Zhao S, Lee P, Lui J, et al. Cloud-based push-styled mobile botnets: A case study of exploiting the cloud to device messaging service [C] //Proc of the 28th Annual Computer Security Applications Conf. New York: ACM, 2012: 119-128

[82] Nicolas F, Liam O, Eric C. W32. Stuxnet Dossier [EB/OL]. 2011 [2016-06-10]. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[83] Bencsáth B, Buttyán L, Félegyházi M, et al. sKyWIper (aka Flame aka Flamer): A complex malware for targeted attacks [EB/OL]. (2012-05-29) [2014-06-10]. https://www.crysys.hu/skywiper/skywiper.pdf

[84] Chien E, OMurchu L, Falliere N. W32. Duqu: The precursor to the next stuxnet [C/OL] //Proc of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET). Berkeley, CA: USENIX Association, 2012 [2016-06-01]. https://www.usenix.org/system/files/conference/leet12/leet12-final11.pdf

[85] GReAT. "Red October" diplomatic cyber attacks investigation [EB/OL]. (2013-01-14) [2016-06-14]. https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/#11

[86] Global Research and Analysis Team. The darkhotel APT a story of unusual hospitality [EB/OL]. 2014 [2016-06-14]. https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf

[87] GData. Uroburos highly complex espionage software with Russian roots [EB/OL]. 2014[2016-06-14]. https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf

[88] Bencsáth B, Pék G, Buttyán L, et al. Duqu: Analysis, detection, and lessons learned [C/OL] //Proc of the ACM European Workshop on System Security (EuroSec). New York: ACM, 2012. [2016-06-11]. http://ns2.humantech.dc.hu/publications/files/BencsathPBF12eurosec.pdf

[89] Kaspersky Lab. The DUQU 2.0 - Securelist. [EB/OL]. (2015-06-11) [2016-06-14]. https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

[90] FireEye. HAMMERTOSS: Stealthy tactics define a Russian cyber threat group [EB/OL]. 2015 [2016-06-14]. https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf

[91] Hultquist J. Sandworm team and the ukrainian power authority attacks [EB/OL]. (2016-01-07) [2016-06-14]. https://www.isightpartners.com/2016/01/ukraine-and-sandworm-team

[92] Tanas S. Satellite Turla: APT command and control in the sky [EB/OL]. (2015-09-09) [2016-06-14]. https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky

[93] Wang Ping, Wu Lei, Cunningham R, et al. Honeypot detection in advanced botnet attacks [J]. International Journal of Information and Computer Security, 2010, 4(1): 30-51

[94] Stinson E, Mitchell J C. Characterizing bots' remote control behavior [M] //Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin: Springer, 2007: 89-108

[95] Karasaridis A, Rexroad B, Hoeflin D A. Wide-scale botnet detection and characterization [J]. HotBots, 2007, 7: 7-7

[96] Bilge L, Balzarotti D, Robertson W, et al. Disclosure: Detecting botnet command and control servers through large-scale netflow analysis [C] //Proc of the 28th Annual Computer Security Applications Conf. New York: ACM, 2012: 129-138

[97] Choi H, Lee H, Lee H, et al. Botnet detection by monitoring group activities in DNS traffic [C] //Proc of the 7th IEEE Int Conf on Computer and Information Technology (CIT 2007). Piscataway, NJ: IEEE, 2007: 715-720

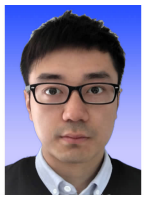
[98] Zhuang L, Dunagan J, Simon D R, et al. Characterizing botnets from email spam records [C] //Proc of the 1st USENIX Workshop on Large-Scale Exploits and Emergent Threats. Berkeley, CA: USENIX Association, 2008

[99] Zhao Yao, Xie Yinglian, Yu Fang, et al. BotGraph: Large scale spamming botnet detection [C] //Proc of the 6th USENIX Symp on Networked Systems Design and Implementation. Berkeley, CA: USENIX Association, 2009: 321-334

[100] MSRT. Tackling the Sefnit botnet Tor hazard [EB/OL]. (2014-01-09) [2016-06-14]. https://blogs.technet.microsoft.com/mmpc/2014/01/09/tackling-the-sefnit-botnet-tor-hazard

[101] Amini P, Pierce C. Kraken botnet infiltration [EB/OL]. (2008-04-28) [2016-06-10]. http://dvlabs.tippingpoint.com/blog/2008/04/28/kraken-botnet-infiltration

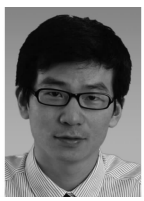
[102] Leder F, Werner T, Martini P. Proactive Botnet countermeasures-an offensive approach [EB/OL]. 2009 [2016-06-10]. http://www.ccdcoe.org/publications/virtualbattlefield/15_LEDER_Proactive_Coutnermeasures.pdf



Li Ke, born in 1988. PhD candidate. His main research interests include information security and machine learning.

Fang Binxing, born in 1960. PhD, professor, PhD supervisor. Member of Chinese Academy of Engineering, fellow member of China Computer Federation. His main research interests include computer architecture, computer network and information security.

Cui Xiang, born in 1978. PhD, professor, PhD supervisor. His main research interests include information security (cuixiang@iie.ac.cn).



Liu Qixu, born in 1984. PhD. Associate professor, master supervisor. His main research interests include network and information security (liuqixu@iie.ac.cn)