doi:10.11959/j.issn.1000-436x.2016118

基于 Webshell 的僵尸网络研究

李可[1,2]，方滨兴[1]，崔翔[1,2]，刘奇旭[2]，严志涛[2]
(1. 北京邮电大学计算机学院，北京 100876；2. 中国科学院信息工程研究所，北京 100093)

摘 要：以 Web 服务器为控制目标的僵尸网络逐渐兴起，传统命令控制信道模型无法准确预测该类威胁。对传统 Webshell 控制方式进行改进，提出一种树状拓扑结构的信道模型。该模型具备普适和隐蔽特性，实验证明其命令传递快速可靠。总结传统防御手段在对抗该模型时的局限性，分析该信道的固有脆弱性，提出可行的防御手段。
关键词：僵尸网络；命令与控制；信道预测；Webshell
中图分类号：TP309.5 **文献标识码**：A

Research on Webshell-based botnet

LI Ke[1,2], FANG Bin-xing[1], CUI Xiang[1,2], LIU Qi-xu[2], YAN Zhi-tao[2]
(1. School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: With the rapid rising of Web server-based botnets, traditional channel models were unable to predict threats from them. Based on improving traditional Webshell control method, a command and control channel model based on tree structure was proposed. The model was widely applicable and stealthy and the simulation experimental results show it can achieve rapid and reliable commands delivery. After summarizing the limitations of current defenses against the proposed model, the model's inherent vulnerabilities is analyzed and feasible defense strategies are put forward.
Key words: botnet, command and control, channel prediction, Webshell

1 引言

僵尸网络（botnet）是指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，被感染的用户终端称之为僵尸主机（bot）；攻击者指掌握僵尸主机资源，对其具有操控权力的控制者（botmaster）；远程控制指攻击者通过命令与控制（C&C, command and control）信道对僵尸主机进行一对多的操控。通过僵尸网络所掌握的大量计算及信息资源，攻击者可发起分布式拒绝服务攻击（DDoS, distributed denial of service）、垃圾邮件（spam）、恶意软件分发、点击欺诈（click fraud）以及比特币网络攻击等恶意活动[2,3]，给互联网安全构成严重威胁。

僵尸网络的发展经历了 3 个阶段：早期僵尸网络以个人计算机 PC 为感染目标；随着智能手机的普及和通信技术的发展，移动僵尸网络逐渐成为了工业和学术研究的新方向。而如今，在 PC 和手机终端防护日趋完善，僵尸主机生存面临瓶颈的背景下，攻击者将目光投向了互联网中大量开放且脆弱的 Web 服务器[4]，根据 NETCRAFT 网站 2015 年 11 月发布的报告[5]显示，全球面向 Web 服务的主机数达 553 万台, Web 站点数量超过 9 亿个。赛门铁克（Symantec）互联网安全威胁研究报告[6]显示，2014 年全球网站中有 76%存在安全漏洞，其中的 20%存在高危漏洞。随着 CGI-PHP（CVE-2012-1823）、Structs2 （CVE 2013-2251）、“破壳”（CVE-2014-6271）等重量级漏洞的频繁曝

收稿日期：2015-12-15；**修回日期**：2016-03-08
基金项目：国家自然科学基金资助项目（No.61303239）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2012AA012902）
Foundation Items: The National Natural Science Foundation of China (No.61303239), The National High Technology Research and Development Program (863 Program)(No.2012AA012902)

出，诸如 Wopbot、TSUNAMI、BoSSaBoTv2 等[7,8]以 Web 服务器为攻击对象的僵尸网络案例不断出现，网站的服务及数据安全面临着严峻的挑战。

在 Web 服务器僵尸网络的研究方向上，学术界尚未出现针对该应用背景的攻防研究。此外，工业界案例普遍存在感染过程复杂、依赖管理员/系统权限、通信信道脆弱的缺陷，难以广泛实现和长期生存。这些已有案例未能针对 Web 服务的特性和对抗环境进行演化，该类型的僵尸网络预测尚存在研究的空间。

基于以上事实，利用 Webshell 构建普适和隐蔽的僵尸网络是一种新思路。如表 1 所示，同 PC 和移动僵尸网络相比，Webshell 僵尸网络在终端防护、权限要求和数据资源上存在差异，可利用 Web 应用或服务漏洞自动化感染网络中大量脆弱目标。此外，由于 Webshell 无法主动持续化运行、依靠外界请求执行功能代码，其命令下需采用主动推送的方式传递（如图 1 和图 2 所示）。上述因素导致了传统中心结构和 P2P 结构僵尸网络模型无法应用于 Webshell 管控。然而，已知的 Webshell 的控制方法在面向大规模场景下存在单点性能瓶颈，各感染节点协同工作能力较差，因此，需要提出一种更加高效和健壮的模型来预测此类僵尸网络威胁。

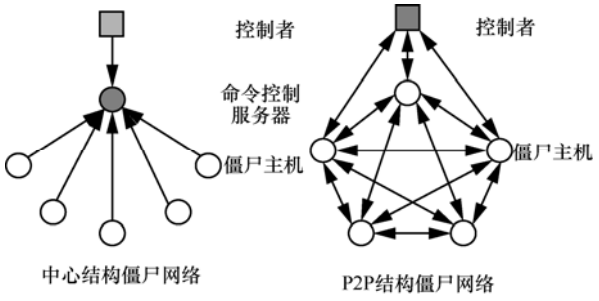


图 1　中心结构和 P2P 结构僵尸网络

基于以上事实，本文提出一种基于树状层次化结构的 Webshell 僵尸网络。该僵尸网络不依赖固脆弱的命令控制资源，引入主机信誉评估和动态加密机制，具有良好的健壮性和隐蔽性。仿真实验证明该僵尸网络的命令传递高效可靠，可管理大规模 Webshell。同时针对该僵尸网络特点，本文提出了可行的防御方法。

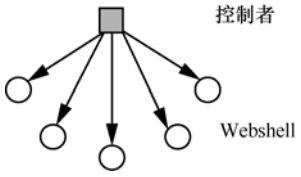


图 2　Webshell 管控拓扑

2　相关工作

为了应对未来新型僵尸网络的威胁，研究人员开展了大量僵尸网络信道模型的预测。其中，非中心结构的僵尸网络具有较好的抗毁能力，成为了研究人员关注的重点。Wang 等[9]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，其初始化（bootstrap）过程不依赖硬编码的节点名单（peer list）或特定域名资源，消除了单点失效，信道的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，具有较好的抗毁能力，可管理大规模僵尸网络。Starnberger 等[10]提出了一种基于 Kademlia 协议的僵尸网络命令控制信道协议 Overbot， 僵尸主机的请求流量隐藏在合法 P2P 应用中，难以被追踪和发现，极大提升了僵尸网络整体健壮性和隐蔽性。Hund 等[11]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僵尸主机验证机制（credit-point system）以及工作量证明机制（proof-of-work）判断通信节点身份的真实性，能有效对抗节点名单污染以及“女巫”（sybil）攻击[12]，具有较好的主机生存性。

表 1　　PC 僵尸网络、移动僵尸网络与 Webshell 僵尸网络对比

网络	僵尸程序运行模式	权限要求	终端防护	感染是否需要用户配合	终端数据资源
PC 僵尸网络	主动持续运行	管理员或系统权限	PC 杀毒软件、防火墙	大多数需要	个人敏感信息，包括登录口令，文档、金融账户信息、邮件等
移动僵尸网络	主动持续运行	安装及敏感功能授权	手机杀毒软件	大多数需要	个人敏感信息，包括手机联系人、短信、邮件等
Webshell 僵尸网络	被动请求执行	Web 站点权限	Web 应用防火墙	否	网站后台数据及主机敏感信息

虽然 P2P 僵尸网络具有良好的健壮性，然而其最大的局限性在于难以管理，因此，一些研究人员尝试对中心结构僵尸网络进行改进，通常采用第三方协议和应用充当通信载体和媒介，以此增强僵尸网络的隐蔽性和健壮性。Singh 等[13]评估了利用 E-mail 实现僵尸网络通信的可行性。Xu 等[14]研究了利用 DNS 来构建隐蔽的命令控制信道的可行性。Xiang 等[15]利用 Web 2.0 服务提出了一种基于 URL Flux 技术的移动僵尸网络，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。Lee 等[16]提出了一种 Alias-Flux 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，实现了隐蔽的命令控制活动。

不同于上述已有工作，本文在对传统 Webshell 改进的基础上，提出一种针对 Web 服务器的轻量级僵尸网络 Webot，该僵尸网络基于 HTTP 协议，不依赖系统权限和第三方应用，具有普适特性；使用主动推送模式下发命令，不依赖脆弱信道资源，较传统信道模型更适用于 Web 服务器管控场景。

3　信道设计与实现

3.1　Webshell 管控模式改进

传统 Webshell 侧重于单点控制，攻击者往往开发私有脚本工具对 Webshell 进行单点批量化管理。然而，该模式本质上是简单且脆弱的，在面向大规模管控时并发能力有限，命令下发耗时较长，难以满足实时协同任务的需求。为了满足大规模场景下高效的命令传递和灵活管控，本文对传统 Webshell 的访问连接及代码结构进行了如下改进。

1) 在访问连接方面，以 PHP 格式的 Webshell 为例，命令传递过程采用无连接思想，即控制者将命令发送给当前僵尸主机后，不等待其执行返回继续执行后续命令下发，*ignore_user_abort*( )函数能保证连接断开后僵尸程序仍可继续正确执行，该方法极大缩短空闲等待时间，允许攻击者实现命令快速传递。

2) 在代码结构方面，传统的 Webshell 主要分为简单 Webshell 和功能 Webshell 2 种形式。

定义 1　简单 Webshell：俗称“小马”，指仅提供基本命令执行功能的 Webshell，代码结构简单。

定义 2　功能 Webshell：俗称“大马”，指包含完整木马功能的 Webshell，代码结构复杂，功能多样。

简单 Webshell 形如 <?php @eval （$_POST["value"]）;?>，不包含复杂功能代码，命令执行时需动态上传完整执行代码，体积较小，常用于上传功能 Webshell；而功能 Webshell 通常将所有的功能代码整合到 Webshell 文件中，命令执行时无需上传执行代码，但存在文件体积较大、易遭遇上传拦截和静态查杀的弊端。本文采用的 Webshell 选取了二者的平衡点，提供基本命令运行及协议实现所需的逻辑功能，不包含具体功能（如 DDoS、扫描等）代码，使僵尸程序在支持复杂控制逻辑、具备良好功能扩展性的同时，仍具有较高的渗透成功率和较好的终端生存性。

3.2　信道拓扑结构

为了消除命令下发单点瓶颈，实现快速、健壮、隐蔽的信息传递，本文设计实现了一种层次化树状拓扑结构的信道模型，该模型自顶向下并发传递命令，其中，Webshell 统一称为僵尸主机，进一步按职能又可划分为超级僵尸主机和普通僵尸主机，两者定义如下。

定义 3　超级僵尸主机：通过信誉评估方法筛选出稳定可信的僵尸主机，该类主机在命令的传递过程中承担命令转发职能，既充当服务端又充当客户端。

定义 4　普通僵尸主机：不可信或不稳定的僵尸主机，在命令传递过程中只等待接收攻击者指令，不承担转发功能，只充当客户端。

如图 3 所示，控制者通过跳板网络[2]将命令传递给超级僵尸主机，超级僵尸主机将接收到的命令消息彼此独立、并发地转发给后续子节点，逐层传递，直到命令传达到所有叶子节点（即普通僵尸主机）为止。

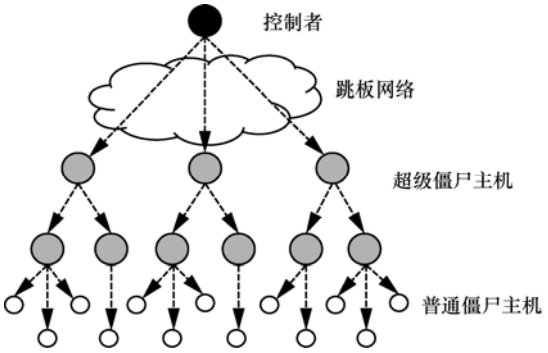


图 3　Webot 僵尸网络拓扑结构

3.3　僵尸主机信誉评估

在 Webot 设计中，为消除不稳定或不可信主机（如 Sybil 节点）对僵尸网络命令控制活动的影响，本文采用信誉评估（reputation evaluation）的方法来对僵尸主机进行筛选，选取可信可靠的主机充当超级僵尸主机，而余下的则为普通僵尸主机，信誉评估标准包括如下内容。

1) 在线时间 T。控制者通过 Call Home 命令对僵尸主机的在线情况进行统计，在线时间越长，认为该主机更稳定可靠。

2) 网站排名 R。假定防御人员部署的 Sybil 节点通常不具备高权重和高排名属性，基于白名单思想，控制者可借助 Alexa 排名识别部分高权重的主机，该类僵尸主机通常被认为是可信的。

3) 工作量证明 P。基于 Sybil 节点不会对真实互联网发动大量恶意攻击的假设，执行大量恶意攻击的僵尸主机将拥有更多的工作量证明，其可信度越高，控制者通过僵尸主机对自主建立的感知节点进行低速攻击（如 DDoS）来评估工作量。

综合上述 3 个因素，单台僵尸主机的信誉值 V_i 的判定如下

$$V_i = w_T T_i + w_R R_i + w_P P_i \tag{1}$$

其中，w_T、w_R、w_P 分别代表上述各对应因素的判断权重，当 V_i 高于预设阈值δ时认为该僵尸主机可充当超级僵尸主机，V_i 越高，所在的层数越小；反之，V_i 低于阈值δ的僵尸主机被判定为普通僵尸主机。

3.4　僵尸主机状态转移设计

每个感染主机均处于等待或活跃 2 类状态：当空闲时，主机处于等待状态，等候外部来自控制者或其父节点的命令；相应地，主机从接收命令开始到执行代码完毕，整个过程称为活跃状态，具体又可分为接受命令、解析命令、攻击、转发、更新 5 个子状态。

如图 4 所示，默认超级僵尸主机处于等待状态，一旦获得外部命令后开始执行解密和分析操作。认证无误后，超级僵尸主机开始执行命令，包括转发、攻击和更新 3 种操作状态：转发操作指超级僵尸主机根据解析的命令内容，将指定的命令转发给选定的子节点；攻击指执行既定的攻击功能（在第 4.5 节具体介绍）；更新操作指下载最新功能插件或更新自身文件。命令执行完毕后，主机回归等待状态，等待接受下一次命令。

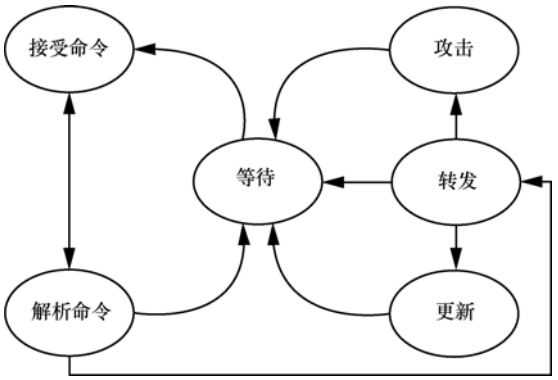


图 4　超级僵尸主机状态转移

如图 5 所示，普通僵尸主机与超级僵尸主机状态转移过程大致相同，不同之处在于，普通僵尸主机只具备攻击和更新 2 种操作状态，不具备转发状态。

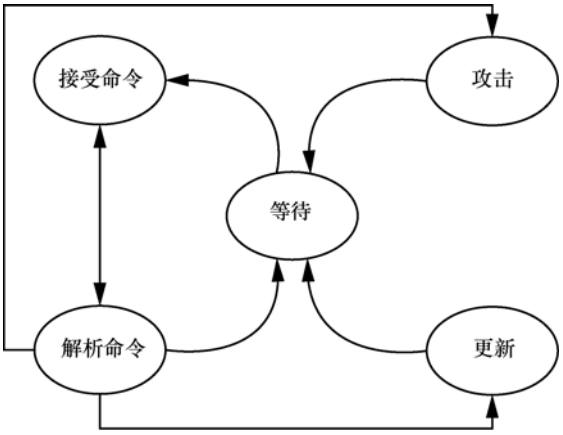


图 5　普通僵尸主机状态转移

3.5　命令控制协议实现

为隐藏 C&C 服务器的真实身份、实现匿名的信息传递，Webot 基于 hidden service 服务，将 C&C 服务器架设在匿名网络 Tor 中[17]，防御人员难以定位其真实 IP。此外，基于可信的云主机或 VPS 资源，利用第三方代理软件（如 Tor2Web），Webot 在 Tor 网络的边界搭建代理节点（如图 6 所示），使公网中的僵尸主机无需安装额外组件即可访问 Tor 网络中的 C&C 服务器。

在协议实现过程中，为了保护通信安全，防止信道劫持，Webot 结合对称加密 RC4 和非对称加密 RSA 2 种方式对命令来源进行鉴别。同时采用动态加密思想，即单个主机单次通信密钥动态变换机制，对僵尸主机请求 C&C 服务器过程进行加密认证。表 2 和表 3 分别描述了协议实现中有关参数及各实体所掌握资源情况。

表 2　　相关参数说明

参数	说明
C_N	通知命令，告知节点请求获取功能或转发命令
C_F	功能命令，包括 DDoS、扫描、垃圾邮件发送、文件回传、Call-Home、更新等
C_T	转发命令，包括转发目标 U 及对应的通知命令 C_N
U	Webot 僵尸主机 URL 列表
IP_{Sensor}	代理节点地址
$E()$	RSA 加密算法
$E'()$	DES 加密算法
Public_Key	RSA 加密算法公钥
Private_Key	RSA 加密算法私钥
ID_i	Bot ID，标识唯一的僵尸主机
T	时间窗，包括开始时间和结束时间
R_Key	一次性会话密钥

表 3　　各实体所掌握资源

角色	所掌握资源
控制者	*Private_Key* ΣC_N ΣR_Key_i ΣC_F
C&C 服务器	U ΣC_N ΣR_Key_i ΣC_T ΣID_i
僵尸主机	*Public_Key* ΣID_i
代理节点	无

如图 6 所示，Webot 命令控制协议实现步骤如下。

1) 控制者事先生成 Σ *R_Key* 集合，利用 *Private_Key* 对通知命令 C_N 加密得到 $E(C_N)$，然后连同待下发的功能命令 C_F 一同部署在 C&C 服务器中。

2) 控制者通过跳板网络将 $E(C_N)$发送给初始的超级僵尸主机，$E(C_N)= E(IP_{Sensor}, R\_Key, T)_{Private\_key}$，其中，$IP_{Sensor}$ 为代理节点的地址；*R_Key* 表示当前僵尸主机当次通信所使用的临时密钥，简称一次性会话密钥；T 标识该命令的有效时间。

3) 超级僵尸主机接收到 $E(C_N)$后利用硬编码的 *Public_Key* 进行解密校验，校验无误后利用 *R_Key* 对自身硬编码的 ID_i 进行加密，将 $E'(ID_i)_{R\_Key}$ 发送给代理节点，代理节点将请求转发给位于 Tor 网络中的 C&C 服务器。

4) C&C 服务器在接收到请求后，对 ID_i 身份及 *R_Key* 的有效性进行校验，校验通过则返回 $E'(C_T, C_F)_{R\_Key}$。

5) 超级僵尸主机对返回的命令 $E'(C_T, C_F)_{R\_Key}$ 进行解密，其中，$C_T=<U_i, E(C_N)> =<U_i, E(IP_{Sensor}, R\_Key, T)_{Private\_Key}>$，超级僵尸主机得到 U_i 后，向其中目标主机转发对应的通知指令 $E(C_N)$，转发完毕执行功能指令 C_F。若后续子节点为超级僵尸主机，则执行上述类似操作；若为普通僵尸主机，则只接受并执行 C_F，不进行转发。

上述通信流程保证了只有合法僵尸主机才能知晓控制者指令，他人无法通过流量监听获取通信内容，保证了通信的机密性。采用 *R_Key* 加 *ID* 的认证方法，能对请求主机身份进行有效鉴别，每个 *R_Key* 只允许当次僵尸主机对 C_T 内容请求一次，可

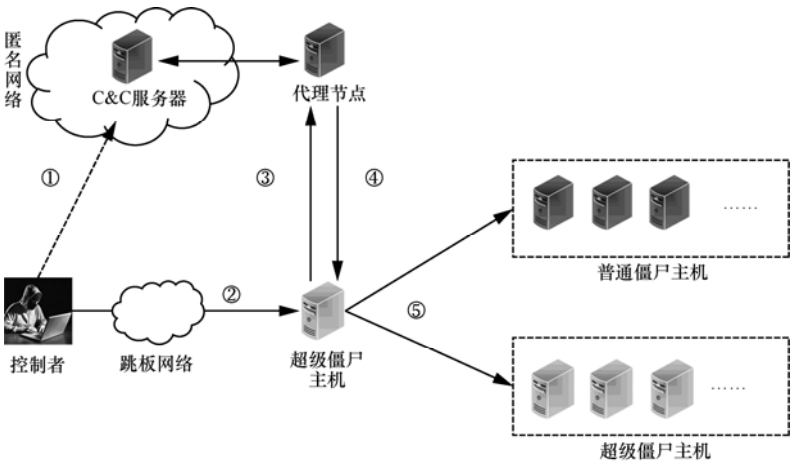


图 6　Webot 命令与控制协议实现

有效防止恶意重复请求。

4 实验评估

为检验 Webot 模型命令传递率及健壮性，本文在仿真环境中对大规模管控场景进行模拟，评估其命令下发速率及传达率；将 Webot 与随机网络和小世界模型[18]进行抗毁能力对比；同时，对 Webot 可实现的功能进行简要评估。

4.1 实验环境

本文在本地 Openstack 虚拟环境下模拟了 3 000 台僵尸主机，其 Web 容器采用 Apache 2.4.2，Webshell 采用 PHP 语言构建，代理节点基于 Nginx 1.9.4 搭建。为了避免实验中产生的恶意流量危害真实互联网，本文将 C&C 服务器设在本地实验环境中，整个通信过程均在本地隔离的环境中完成。

4.2 效率评估

基于单线程模式及相同的网络参数设置，本文对传统 Webshell 下发模式（下文简称传统模式）和 Webot 协议进行命令下发比较实验：在传统模式实验中，以单点逐一下发的方式将攻击者指令直接传递给所有僵尸主机，信息传递超时时间设置为 3 s；在 Webot 信道模拟实验中，相比于前者，该传递过程增加了 C&C 服务器请求环节，考虑到在实际下载和转发过程会产生较为明显的耗时，根据预先真实网络中测试结果，在本地仿真实验中设置 5 s 休眠来模拟真实网络延迟。每一个超级僵尸主机在接收到命令后将指定命令转发给后继的 N 个僵尸主机，源主机在发送数据分组后不等待当前目标主机的反馈和代码执行，直接执行下一个目标主机的转发。C&C 服务器可根据僵尸主机请求实时掌握全网命令传递情况。

图 7 显示了下发成功数随时间变化的情况。假设每个超级僵尸主机转发给 5 个子节点(N = 5)。在最初下发的 36 s 中，传统模式下发速率比 Webot 的速度快，这是由于初始阶段 Webot 的并发数量少、请求延迟高造成的。在 36 s 之后，随着并发的超级僵尸主机数量的不断增多，命令传达速度不断提高，发送成功数呈指数级上升，超过了线型增长的传统模式，且随时间的推移，两者数量的差距逐渐拉大。在整个 Webot 下发实验中，除去少量僵尸主机因网络阻塞原因造成的接收失败，共计 2 915 台僵尸主机在 116 s 内完成了命令传递；相比之下，传统模式在同样时间内只下发了 323 台僵尸主机。可见 Webot 的管控效率较传统模式具有巨大优势。

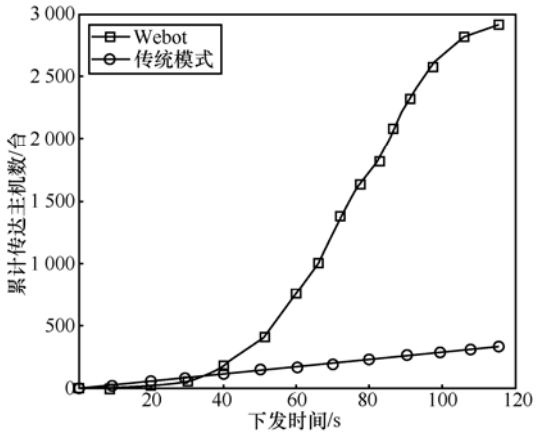


图 7 命令下发数量对比

4.3 可靠性评估

当 Webot 拥有高速下发速率的同时，它的传递可靠性也同样保持较高的水平，本文用命令传达率来评估 Webot 协议自身传递的可靠性。假设每个超级僵尸主机转发成功率 Q 为 0.9，这意味着每一个后续节点有 0.9 的概率能正确接收到命令。参数 L 代表转发路径的深度。S_{All} 代表僵尸主机总数，S_{Received} 代表成功接收到指令的数，Webot 的命令传达率 C 为

$$C=\frac{S_{\mathrm{Received}}}{S_{\mathrm{All}}}=\frac{1-N}{1-N^{L}}\sum_{i=1}^{L}(NQ)^{i-1} \tag{2}$$

如图 8 所示，转发数 N 分别设为 10、20、50，在同等条件下进行模拟实验，同等规模下 N 值越大，层数 L 越小，传达率 C 越高。选取 N 为 50，模拟 100 000 台的大规模管控场景，当 Webot 采用不重传策略时，其全网一次性传达率为 73.11%；通过感知全网下发情况，对未到达节点进行 2 次下发，其全网信息传达率可达 93.10%，累计下发耗时约 750 s。

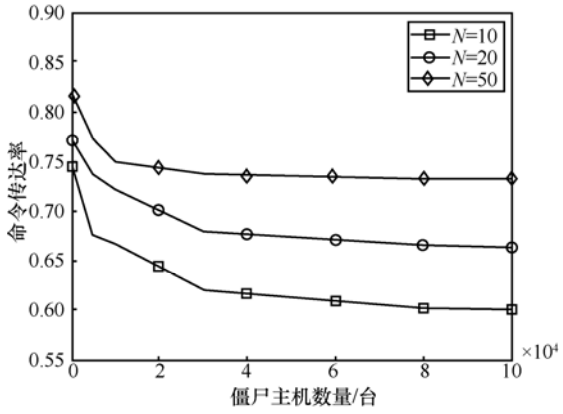


图 8 Webot 命令传达率评估

4.4　抗毁能力评估

本文采用 Li 等[18]提出的评估方法，随机去除一定数量主机后观察剩余主机的命令可达情况，即最大剩余可达率（如式（3）所示）。对比随机网络模型、小世界网络模型以及 Webot 模型三者的抗毁能力。

$$\text{最大剩余可达率}=\frac{\text{命令传达主机数}}{(\text{僵尸主机总数}-\text{僵尸主机移除数})} \tag{3}$$

实验选取的随机网络模型其平均邻居节点数为 2，小世界网络模型的平均邻居节点数设为 4，在同等 10 000 台规模下进行测试。如图 9 所示，Webot 的抗毁能力明显优于随机网络模型。当移除数小于约 2 500 台时，Webot 的最大剩余可达率略低于小世界网络模型。随着移除数的进一步增加，小世界网络模型的连通性能下降明显，而 Webot 的下降较为平稳，仍能保持一定的可达率。除此之外，Webot 信道具有易恢复和可重构特性，因此，认为该模型具有较好的健壮性。

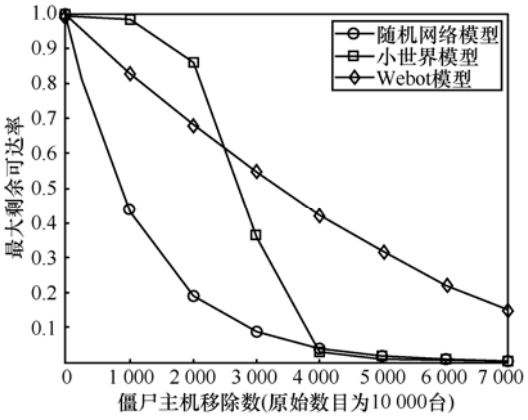


图 9　3 种模型的最大剩余可达率对比

4.5　功能评估

Webot 信道模型兼容传统 Webshell 的管控功能，具备传统文件上传、数据库管理等基本功能。此外，控制者可利用 Webot 实现其他复杂的恶意攻击。

1) DDoS。利用 Webot 高效和协同特性，控制者可以在短时间内集结全网僵尸主机实施持续化的 DDoS 攻击，由于 Web 服务器资源往往具有高带宽性能，通常认为该类僵尸网络较传统 PC 僵尸网络破坏性更强。本文通过网络靶场中 60 台志愿者主机对 Webot 的 DDoS 能力进行实际测试，如图 10 所示，DDoS 最高峰值可达 6 755 kbit/s，同等条件下，1×10^5 台规模 DDoS 峰值流量理论上可达 10.73 Gbit/s。

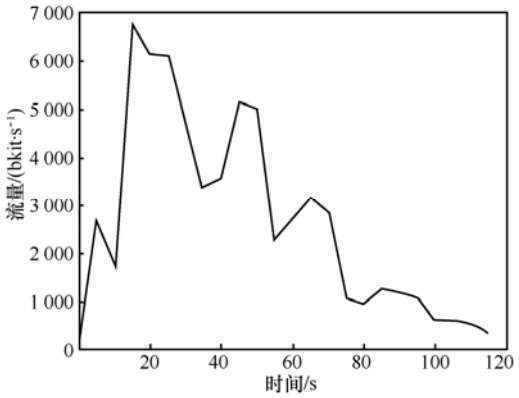


图 10　Webot DDoS 流量记录

2) 网络空间探测。利用分布的 IP 和计算资源，结合主控端的统一调度，Webot 可用于全球网络空间设备探测，有效解决了探测过程中 IP 遭遇封锁的问题。

3) 钓鱼攻击。Webot 掌握了丰富的合法域名资源，通过篡改页面的方式，攻击者可实施持续性的钓鱼攻击。

4) 黑帽搜索引擎优化。根据 Wang 等[19]的研究显示，小规模、低流失率的黑帽搜索引擎优化（Black Hat search engine optimization）僵尸网络可对谷歌搜索结果进行毒化，实现恶意内容推广，为攻击者牟取巨额利益。Webot 同样可以实现该功能。

5　防御分析

5.1　传统防御方法缺陷

传统僵尸网络的防御方法包括 Sybil 攻击、Sinkhole 攻击[20]、劫持以及爬取攻击等，通过这些方法防御人员可以对僵尸网络进行测量、干扰和关闭。本文提出的 Webot 可以有效抵御这些常规方法。

Sybil 攻击。Sybil 攻击对于 Webot 的效果十分有限。一方面，在面向大规模僵尸网络的对抗中，由于每个节点所知晓的僵尸主机数有限，防御人员依靠少量 Sybil 节点很难测量整体的活跃数和规模数；另一方面，即使 Sybil 节点拒绝将消息转发给后续节点，企图切断命令传递通道，控制者仍可迅速发现该异常，对未接收消息的主机实行二次下发，同时将 Sybil 节点从超级僵尸主机列表中剔除。

Sinkhole 攻击。通过前期渗透植入，控制者掌握了全网僵尸主机信息，通过主动推送方式将 C&C 资源告知全网僵尸主机。该类资源可灵活更替且实现成本小，防御人员难以提前预测并控制这些资源。此外，Tor 网络能有效保护 onion 域名解析过程的安全。因此，Sinkhole 手段对于 Webot 而言几乎无效。

劫持。同其他僵尸网络类似，Webot 采用非对称加密算法和时间窗机制来校验命令的有效性，防止命令欺骗和重放攻击，理论上防御人员无法劫持该僵尸网络。

爬取攻击。安全人员试图通过爬取的方式发掘僵尸网络的拓扑信息。在 Webot 模型中，他们可能利用捕获的僵尸主机重复发送请求来获取大量主机信息。然而，在僵尸主机访问 C&C 服务器过程中，服务器的验证机制首先会检查 bot *ID* 和 *R_Key* 的有效性。防御人员通过逆向分析事先获取了合法的 bot *ID*，如果缺少合法 *R_Key* 将无法通过验证。即使利用 *Public_Key* 对通信内容破解，掌握了一次性会话密钥 *R_Key*，也只允许获得一次主机信息 *U*，再次提交将会被拒绝。除非能够绕过信誉评估机制并控制大量超级僵尸主机资源，否则，该种攻击效果是有限的。

5.2 Webot 防御手段

针对 Webot 的实现机理，本文介绍 4 种有效的防御手段。首先，匿名网络的自身缺陷可导致僵尸网络被测量和去匿名化；其次，防御人员可通过渗透手段对僵尸网络恶意行为进行实时监控；第三，可对通信过程中的代理节点实施分布式拒绝服务攻击；最后，防御人员需要建立一个国际性的合作渠道来识别、追踪和防御 Webot。

利用匿名网络漏洞。如果 Webot 所使用的匿名网络存在可被利用的漏洞，这将影响 Webot 的整体健壮性和匿名性。以 Tor 网络为例，安全防御人员可通过控制 hidden service 的 guard node 来进行流量的聚合分析[21]，揭示 C&C 服务器的真实 IP。

渗透监控。由于僵尸主机均需要访问 C&C 服务器来获取完整代码和指令，对于 Webot 而言，安全人员控制少量僵尸主机实施隐蔽的渗透攻击是无法避免的。该方法可持续追踪分析僵尸网络的活动。

代理节点拒绝服务攻击。在 C&C 通信过程中，防御人员对代理节点进行拒绝服务攻击，可干扰僵尸网络的命令传递，延长全网命令传达时间，降低其协同攻击的效果。

构建国际合作机制。Webot 的实现需要匿名网络和虚拟主机提供服务，防御人员应该努力提高公共可用服务的安全性，避免这些服务被恶意利用。同时应该建立一个包含安全研究机构、CERT 以及 ISP 在内的协作渠道来共同打击此类僵尸网络犯罪。

6 结束语

本文设计了一种基于 Webshell 的树状拓扑结构僵尸网络模型并实现了其原型系统 Webot。该僵尸网络可面向大量脆弱 Web 服务和应用构建，具有良好普适性。基于匿名网络保护，结合主机信誉评估机制，防御人员难以追踪；命令传递采用主动下发，不依赖固定且脆弱集合点，信道难以被关闭。本地仿真实验证明了 Webot 模型具有良好的效率及健壮性，代表了未来僵尸网络的发展趋势，预计类似的实际案例将会在不久的将来出现。在下一步工作中，将针对该类型的僵尸网络进行深入研究，寻找快速有效的检测方法。

参考文献：

[1] CUI X, FANG B X, et al. Botnet triple-channel model: towards resilient and efficient bidirectional communication botnets[M]//Security and Privacy in Communication Networks. Springer International Publishing, 2013.

[2] SHAHID K, et al. A taxonomy of botnet behavior, detection, and defense[J]. Communications Surveys & Tutorials, IEEE 2015, 16(2): 898-924.

[3] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on Bitcoin's peer-to-peer network[C]//24th USENIX Security Symposium (USENIX Security 15). c2015: 129-144.

[4] CANALI D, BALZAROTTI D. Behind the scenes of online attacks: an analysis of exploitation behaviors on the Web[C]//20th Annual Network & Distributed System Security Symposium (NDSS 2013). c2013.

[5] Netcraft. Web server survey[EB/OL]. http://news. netcraft.com/archives/2015/11/16/november-2015-web-server-survey.html.

[6] Symantec. 2015 Internet security threat report [EB/OL]. https://www.symantec.com/security_response/publications/threatreport. jsp.

[7] F-Secure. Backdoor: Osx/tsunami[EB/OL]. https://www. f-secure.com/v-descs/backdoor_osx_tsunami_a.shtml.

[8] New bot malware (BoSSaBoTv2) attacking Web servers discovered[EB/OL]. https://www.trustwave.com/Resources/SpiderLabs-Blog/-Honeypot-Alert--New-Bot-Malware-(BoSSaBoTv2)-Attacking-Web-Servers-Discovered/.

[9] WANG P, SPARKS S, ZOU C C. An advanced hybrid peer-to-peer botnet[J]. IEEE Transactions on Dependable and Secure Computing, 2010, 7(2): 113-127.

[10] STARNBERGER G, KRUEGEL C, KIRDA E. Overbot: a botnet protocol based on Kademlia[C]//The 4th International Conference on Security and Privacy in Communication Networks. ACM, c2008.

[11] HUND R, HAMANN M, HOLZ T. Towards next-generation botnets[C]// European Conference on Computer Network Defense. IEEE, c2008: 33-40.

[12] DOUCEUR J R. The sybil attackpeer-to-peer systems[M]//Springer Berlin Heidelberg, 2002: 251-260.

[13] SINGH K, SRIVASTAVA A, GIFFIN J, et al. Evaluating email's

feasibility for botnet command and control[C]// IEEE International Conference on Dependable Systems and Networks With FTCS and DCC, IEEE, 2008: 376-385.

[14] XU K, BUTLER P, SAHA S, et al. DNS for massive-scale command and control[J]. IEEE Transactions on Dependable and Secure Computing, 2013, 10(3): 143-153.

[15] CUI X, FNAG B X, et al. Andbot: towards advanced mobile botnets[C]//Proceedings of the 4th USENIX Conference on Large-Scale Exploits and Emergent Threats. USENIX Association, c2011: 11-11.

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

[17] SANATINIA A, NOUBIR G. OnionBots: subverting privacy infrastructure for cyber attacks[C]//Dependable Systems and Networks (DSN), c2015: 69-80.

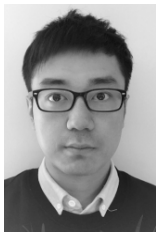
[18] LI J, EHRENKRANZ T, KUENNING G, et al. Simulation and analysis on the resiliency and efficiency of malnets[C]//Principles of Advanced and Distributed Simulation. IEEE, c2005: 262-269.

[19] WANG D Y, SAVAGE S, VOELKER G M. Juice: a longitudinal study of an SEO botnet[C]//The NDSS Symposium. c2013.

[20] STONE-GROSS B, COVA M, CAVALLARO L, et al. Your botnet is my botnet: analysis of a botnet takeover[C]//The 16th ACM Conference on Computer and Communications Security. ACM, c2009: 635-647.

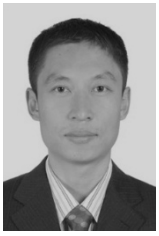
[21] BIRYUKOV A, PUSTOGAROV I, WEINMANN R. Trawling for tor hidden services: detection, measurement, deanonymization[C]// 2013 IEEE Symposium on Security and Privacy (SP). c2013: 80-94.

作者简介：

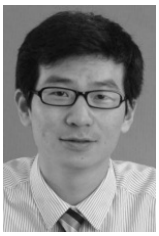


李可（1988-），男，湖南益阳人，北京邮电大学博士生，主要研究方向为网络安全。

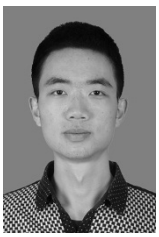
方滨兴（1960-），男，江西万年人，中国工程院院士，北京邮电大学教授、博士生导师，主要研究方向为计算机体系结构、计算机网络与信息安全。



崔翔（1978-），男，黑龙江讷河人，博士，中国科学院信息工程研究所研究员，主要研究方向为网络安全。



刘奇旭（1984-），男，江苏徐州人，博士，中国科学院信息工程研究所副研究员，主要研究方向为网络空间安全评测。



严志涛（1991-），男，浙江临海人，中国科学院信息工程研究所硕士生，主要研究方向为网络安全。