

## 僵尸网络综述

孙彦东, 李 东

(哈尔滨工业大学 国家计算机网络与信息内容安全重点实验室, 黑龙江 哈尔滨 150001)

(sunyandong@pact518.hit.edu.cn)

**摘 要:**僵尸网络(Botnet)是由 Bot 组成的可通信、可被攻击者控制的网络。Botnet 对今天网络构成越来越大的威胁,由于组成 Botnet 的主机数量非常庞大,由 Botnet 发起的攻击的破坏性非常惊人。介绍了 Botnet 的定义、历史及所带来的危害,同时介绍了研究 Botnet 的方法,并给出了应对 Botnet 的措施,最后简要地论述和分析了 Botnet 的变化趋势。

**关键词:**僵尸网络; IRC; 分布式拒绝服务; 蜜罐

**中图分类号:** TP393.08 **文献标识码:** A

## Overview of Botnet

SUN Yan-dong, LI Dong

(Research Center of Computer Network and Information Content Security Technology, Harbin Institute of Technology, Harbin Heilongjiang 150001, China)

**Abstract:** The Botnet is a network which is composed of bots. All bots can communicate with the attacker and are controlled by it. The Botnet has become a tremendous threat of our Internet. The damage of the Botnet is very serious, because the number of PCs of the Botnet is very large. The definition, the history and the damage caused by the Botnet were described. Several methods for studying the Botnet were introduced and the measures to cope with it were given. The trends of the Botnet were analyzed briefly

**Key words:** Botnet; IRC; Distributed Denial of Service(DDoS); Honeypot

## 0 引言

近些年来,利用 Botnet 发送垃圾邮件和进行 DDoS<sup>[1]</sup> 攻击的事件越来越多,Botnet 的问题逐渐受到人们的重视。

Bot 是“Robot”的缩写,是指能够按照预定义的指令执行操作,具有一定智能的程序<sup>[2]</sup>。同目前流行的恶意代码如蠕虫、木马、病毒和间谍软件相比,Bot 具有不传播性、高度可控性、窃密性等特点。第一个 Bot 是 1993 年的 Eggdrop Bot,它运行在 Unix 环境下。1999 年 11 月出现的 SubSeven 2.1 木马成功地运用 IRC(Internet Relay Chat)协议控制了感染该木马的主机。

Bot 的种类很多,其中攻击者利用最广泛的是 IRC Bot,它利用 IRC<sup>[3]</sup> 协议相互通信,同时攻击者利用该协议进行远程控制。在 IRC Bot 被植入被攻击者主机后,它会主动连接 IRC 聊天服务器,接受攻击者的命令。Gibot 就是一种 IRC Bot,此外还有 AOL Bot, P2P Bot<sup>[2]</sup>。目前也有一些被人们使用的良性 Bot,如搜索引擎 Bot、聊天 Bot、游戏 Bot 等。

Botnet(僵尸网络)是由一组被植入受控 Bot 的主机(Zombie)所组成的网络结构,目前所指的 Botnet 都是基于 IRC 的 Botnet。当攻击者利用某种漏洞或蠕虫攻陷一台主机后,就会把 IRC Bot(僵尸工具)<sup>[4]</sup> 植入该主机,IRC Bot 就会自动按照预先设定的命令连接 IRC 服务器中的固定频道(channel)等候攻击者发布命令。这些能够在一个 IRC 频道被远程控制的主机就组成了 IRC Botnet(以下称 Botnet)。

## 1 Botnet 结构、形成及功能

### 1.1 Botnet 结构

Botnet 的典型结构如图 1<sup>[5]</sup>。被安装在主机中的 Bot 能够把自己拷贝到一个安装目录,并能够改变系统配置,以便开机就能够运行。攻击者应用事先设定的用户名和密码登录到指定的 IRC 服务器中的固定频道,其中 IRC 服务器可能是由服务提供商提供,或者是被攻陷的主机,向所有连接到该频道的 Bot 发布命令。

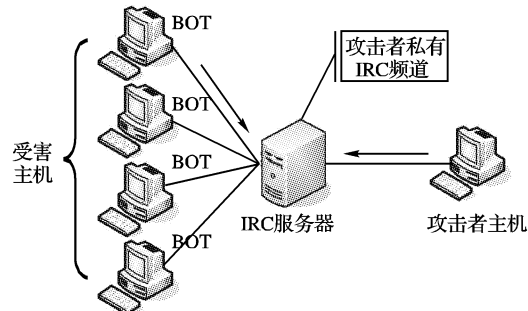


图 1 Botnet 结构

### 1.2 Botnet 的形成及控制

攻击者首先通过加入扫描和攻陷漏洞程序精心编写新的 Bot 或者修改能够得到的 Bot 来获得将要投放的 Bot,这些 Bot 能够模拟 IRC 客户端与 IRC 服务器进行通信;然后利用 Bot 扫描某段网络,一旦发现目标,便对目标进行探测和攻击,通常扫描的端口如表 1<sup>[6]</sup>。

收稿日期:2006-01-01;修订日期:2006-03-06

作者简介:孙彦东(1978-),男,黑龙江五常人,硕士研究生,主要研究方向:网络信息与安全;李东(1967-),男(回族),河北沧州人,教授,博士,主要研究方向:网络信息安全技术、并行计算、计算机系统结构、计算机图形学。

表1 端口服务对照表

端口	相关服务	端口	相关服务
TCP/80	Http	UDP/137	NetBIOS
TCP/139	CIFS	UDP/1434	MS SQL Server
TCP/445	CIFS		

攻击者利用被扫描主机的漏洞,通常这个过程利用某种蠕虫进行攻击,获得管理员权限。如果成功攻陷主机,攻击者把编写好的 Bot 工具利用 TFTP,FTP,HTTP 或者 DCC SEND (IRC 用来给其他用户发送文件)上传到主机。Bot 成功安装后,它就会连接预先设定的 IRC 服务器,使用设定的用户名和密码加入特定的频道,等待命令,一般 Bot 把频道的主题解释成命令。有时,攻击者为了防止某一个频道被发现,利用 dyndns.com 或 no-ip.com 提供的服务,把 IRC 服务器映射到动态 IP,让 Bot 加入动态的频道或者多个频道。攻击者用复杂的有时加密的密码登录到频道,发布命令实施各种攻击活动。典型的命令<sup>[4]</sup>如:

1) advscan lsass 200 5 0 -r -s;

2) . http. update http:// < server > / ~ mугenxu/rBot. exe c:\msy32awds. exe 1;

第一条指令命令 Bot 利用 LSASS 漏洞并发运行 200 线程进行进一步扩散;第二条指令用频道的主题指导 Bot 从 Web 上下载一个二进制文件并执行;如果攻击者没有发布任何指令, Bot 则在频道中沉默,等待命令。整个过程可以描述如图 2<sup>[5]</sup>。

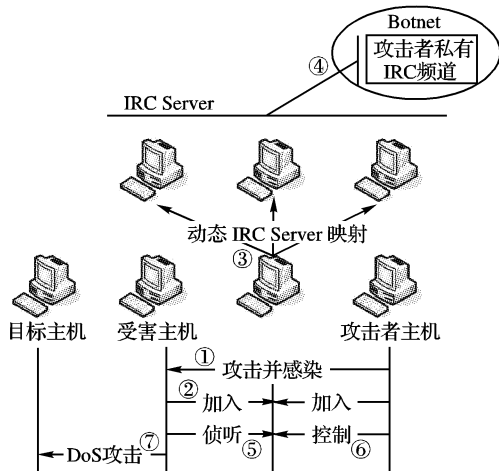


图2 Bot 感染和控制过程

- ① Bot 感染;
- ② 连接 IRC Server;
- ③ 动态域名映射;
- ④ 加入私密频道;
- ⑤ Bot 监听频道,等待指令;
- ⑥ 攻击者进入频道并发出控制指令;
- ⑦ 所有 Bot 根据指令对目标发起攻击。

### 1.3 Botnet 的危害

#### 1) 分布式拒绝服务攻击

这可能是攻击者利用 Botnet 进行的最主要的破坏活动。攻击者利用组成 Botnet 的 Bot 向目标发送大量的 UDP 包、ICMP 请求或者 TCP SYN 请求,消耗带宽,造成目标服务器或主机不能够正常响应合法请求,导致服务缺失。

Botnet 进行 DDoS 攻击大都针对大型的网站,或受雇于某一机构对商业竞争对手实施攻击。

#### 2) 垃圾邮件

Bot 攻陷主机之后,收集主机邮件地址列表,并打开 SOCK v4/v5 代理<sup>[4]</sup>,向邮件列表中的地址发送欺骗邮件或者带有病毒连接的垃圾邮件,造成进一步的危害。由于控制的 Bot 数量庞大,且地址分散,所以很难监测,造成巨大的危害。

#### 3) 扩散恶意软件

Bot 被植入受害主机后,可以从网络上指定位置下载病毒或者其他的恶意软件,如后门软件和木马程序等,造成进一步的感染,同时 Bot 可以扫描受害主机所在的局域网,发现漏洞并上传本身和其他的恶意软件。

#### 4) 窃取敏感信息

被 Bot 控制的主机完全受控于攻击者,攻击者可以通过上传一些间谍软件和监听软件,如 key logger 等,来收集和记录受害主机上的敏感信息,如银行密码、信用卡账号密码等。

除了上述危害外,僵尸网络还被用来安装广告条、攻击 IRC 聊天网络、在线投票和游戏<sup>[4]</sup>和存储非法文件等<sup>[5]</sup>。

## 2 研究 Botnet 的方法及应对措施

### 2.1 Botnet 的传播模型

到目前为止,关于 Botnet 传播特性的研究较少,文献[7]应用时区对 Botnet 传播进行建模,利用 Botnet 的集中控制(C&C)机制收集数据。采用传统方式——honeypot,控制 C&C 服务器的 DNS 服务,使流量导入到 sinkhole (运行 tarptits<sup>[8,9]</sup>,honeypots 和 lightweight responders<sup>[10,11]</sup>的数据收集中心)。Sinkhole 的重定向的实施通过:

1) 应用捕获到的 malware (通过 honeypot, spam filter, honeyd 和其他方式获得)确定 C&C 服务器地址、名称等。

2) 确定 DNS Start of Authority (SOA) for C&C。联系 DNS 注册机构,或者停止 DNS,或者提供一个 A-Rec 给 sinkhole。

通过观察 Botnet,发现在不同的网络,不同的时区,Botnet 活动是有差异的,如图 3<sup>[8]</sup>。

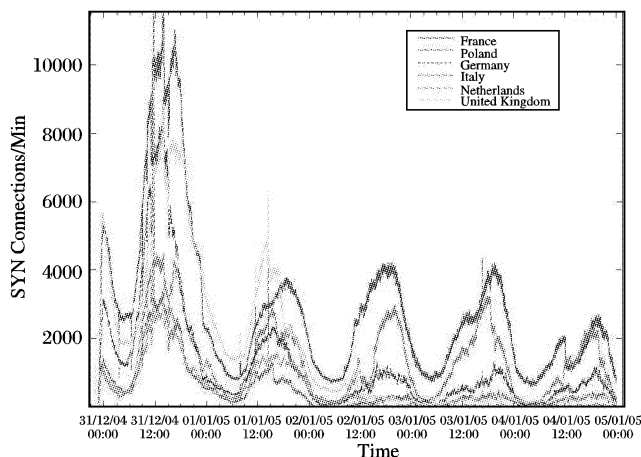


图3 Botnet 活动地理分布

通过分析采集的数据,得出两个 Botnet 的传播模型,单一时区每日模型 (Diurnal Model for a Single Day) 和多时区每日模型 (Diurnal Model for Multiple Time Zones)<sup>[7]</sup>。通过这个模型,可以:1) 预测 Botnet 的未来传播特性,特别是利用相似漏洞传播的 Botnet 的特性,为应对 Botnet 提供依据;2) 划分利用投放时间和区域来加快传播速度的 Botnet 的优先级,做到合理分配资源,集中处理破坏性大的 Botnet。

### 2.2 Botnet 的跟踪方法

借助于蜜网 (Honey Net)<sup>[12]</sup>,可按以下步骤跟踪 Botnet: 首先收集 Botnet 的相关信息,这可以通过分析捕获的恶意软



$$\begin{aligned}
&= e\left(H_2(m), \sum_{i=1}^n f_i(0)P\right) \\
&= e\left(H_2(m), \sum_{i=1}^n (s + H_1(m_\omega, U)k_i + x_i)P\right) \\
&= e\left(H_2(m), (H_1(m_\omega, U)U + Y_0 + \sum_{i=1}^n Y_i)\right)
\end{aligned}$$

## 4 对改进方案的密码分析

### 4.1 安全性

下面分析改进方案克服了原方案的安全隐患,并且满足门限代理签名的其他安全要求。

**定理 1** 改进方案可以抵抗本文提出的伪造攻击和公钥替换攻击。

**证明:** 改进方案的完整有效门限代理签名为  $\langle m, U, m_\omega, \sigma \rangle$ , 删除了原门限代理签名方案签名  $\langle m, U, m_\omega, \sigma' \rangle$ ,  $K >$  中的多余参数  $K$ , 因此避免了针对参数  $K$  的伪造攻击。

改进方案也可抵抗公钥替换攻击, 因为若攻击者(不妨设为代理签名人  $p_1$ ) 欲通过公钥替换攻击的方法伪造对消息  $m'$  的有效门限代理签名,  $p_1$  必须首先任选  $U' \in G_1, l \in Z_q^*$ , 计算:  $Y_1' = lP - (\sum_{j=2}^n Y_j + Y_0 + H_1(m_\omega, U')U')$ ,  $\sigma' = lH_2(m')$ 。

接着必须要求 CA 把他的公钥改为  $Y_1'$ , 但是在改进方案中 CA 要求  $p_1$  必须提供知道公钥  $Y_1'$  对应的私钥  $x_1'$  的零知识证明。由于在群  $G_1$  中, 离散对数问题在计算上是不可行的, 所以  $p_1$  不能求出公钥  $Y_1'$  对应的私钥  $x_1'$ , 也就不能提供知道公钥  $Y_1'$  对应的私钥  $x_1'$  的零知识证明, 因此不能伪造对消息  $m'$  的有效门限代理签名  $\langle m', U', m_\omega, \sigma' \rangle$ 。所以原始签名人  $p_0$  或任何代理签名人  $p_i (1 \leq i \leq n)$  都不能通过公钥替换攻击的方法伪造对任意消息  $m'$  的有效门限代理签名  $\langle m', U', m_\omega, \sigma' \rangle$ 。证毕。

**强不可伪造性** 攻击者伪造的对消息  $m'$  的签名  $\langle m', U', m_\omega, \sigma' \rangle$  要想通过接收者验证, 必须使  $\langle m', U', m_\omega, \sigma' \rangle$  满足验证方程:

$$e(P, \sigma') = e\left(H_2(m'), H_1(m_\omega, U')U' + Y_0 + \sum_{i=1}^n Y_i\right)$$

由于在群  $G_1$  中, 离散对数问题在计算上是不可行的,  $H_1(\cdot), H_2(\cdot)$  为两个强无碰撞安全单向 Hash 函数, 并且  $e$  为一个安全的双线性对, 因此已知  $\langle U', m_\omega, \sigma' \rangle$  之中的任何两个, 去求第三个在计算上都是不可行的, 因此改进方案满足强不可伪造性。

同原方案一样, 改进方案使用了授权书  $m_\omega$ , 并且授权书

$m_\omega$ 、原始签名人和代理签名人的公钥都要在代理签名的验证过程中出现, 因此满足门限代理签名的可验证性、可区分性等其他安全性要求。

### 4.2 性能

表 1 列举了改进方案和原方案在每个阶段所需计算量的比较。令  $A_m, M_m, I_m, A, S$  和  $P$  表示模加运算、模乘运算、求逆运算、点加、数乘运算和双线性对运算。

表 1 计算复杂性比较

运 算	代理密钥生成阶段		代理签名生成阶段		签名验证阶段	
	原方案	改进方案	原方案	改进方案	原方案	改进方案
$A_m$	$2 + n(1 + nt)$	$1 + n(1 + nt)$	0	0	0	0
$M_m$	1	1	0	0	0	0
$I_m$	1	1	0	0	0	0
$A$	$2 + n(t - 1)$	$2 + n(t + n + 2)$	$t + n - 2$	$t - 1$	$n + 2$	$n + 1$
$S$	$2 + n(2t + 5)$	$n(t + n + 1)$	$2t + n$	$2t$	1	1
$P$	$2n$	$2n$	$2t$	$2t$	2	2

从表 1 容易看出, 改进方案在代理密钥生成阶段的计算量大于原方案, 但在代理签名生成阶段和验证阶段计算量比原方案低, 总的来说改进方案计算复杂性略高于原方案。但改进方案所需的通信量比原方案稍低。

### 参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegating signing operation[A]. Proceedings of the 3rd ACM Conference on Computer and Communications Security[C]. New Dehi, India: ACM Press, 1996. 48 - 57.
- [2] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: delegation of the power to sign messages[J]. IEICE Transactions Fundamentals, 1996, E79A(9): 1338 - 1354.
- [3] ZHANG K. Threshold proxy signature schemes[A]. Proceedings of the First International Workshop on Information Security[C]. Berlin: Springer-Verlag, 1997. 191 - 197.
- [4] KIM S, PARK S, WON D. Proxy signatures, revisited[A]. Proceedings of International Conference on Information and Communications Security[C]. Berlin: Springer-Verlag, 1997. LNCS1334. 223 - 232.
- [5] SUM HM, LEE NY, HWANG T. Threshold proxy signatures[J]. IEEE Proceedings of Computers & Digital Techniques, 1999, 146 (5): 259 - 263.
- [6] 李继国, 曹珍富. 一个改进的门限代理签名方案[J]. 计算机研究与发展, 2002, 39(11): 1513 - 1518.
- [7] 钱海峰, 曹珍富, 薛庆水. 基于双线性对的新型门限代理签名方案[J]. 中国科学(E), 2004, 34 (6): 711 - 720.

(上接第 1630 页)

- [9] LISTON T. Welcome to my tarpit - the tactical and strategic use of labrea [EB/OL]. <http://www.hackbus ters.net/LaBrea/LaBrea.txt>, 2001.
- [10] PROVOS N. A virtual honeypot framework [R/OL]. [http://www.citi.umich.edu/techrepts/reports/re ports/citi-tr-03-1.pdf](http://www.citi.umich.edu/techrepts/reports/citi-tr-03-1.pdf), 2003.
- [11] KREIBICH C. Honeycomb automated ids signature creation using honeypots [EB/OL]. <http://www.cl.cam.ac.uk/.cpk25/honeycomb/>, 2003.
- [12] The HoneyNet Project [EB/OL]. <http://www.honeynet.org>, 2005.
- [13] MEADOWS C. A formal framework and evaluation method for network denial of service[A]. Proceedings of the 1999 IEEE Computer Security Foundations Workshop[C]. IEEE Computer Society Press, 1998.
- [14] FREILING FC, HOLZ T, WICHESKI G. Botnet tracking: exploring a root-cause methodology to prevent distributed denial-of-service attacks [Z]. Aachener Informatik Berichte, RWTH Aachen, 2005.
- [15] 诸葛建伟. Botnet 简介[R/OL]. <http://www.icst.pku.edu.cn/honeynetweb/honeynetcn/TechnicalReports.htm>, 2005 - 05.