基于组行为特征的恶意域名检测

张永斌 陆 寅 张艳宁

(西北工业大学计算机学院 西安 710129)

摘 要 目前,僵尸网络广泛采用域名变换技术,以避免域名黑名单的封堵,为此提出一种基于组行为特征的恶意域名检测方法。该方法对每个检测周期内网络中主机请求的新域名集合、失效域名集合进行聚类分析,并将请求同一组新域名的主机集合作为检测对象,通过分析集合内主机在请求失效域名、新域名行为上是否具有组特性,提取出网络中的感染主机集合、C&C服务器使用的IP地址集合。对一ISP域名服务器监测的结果表明,该方法可准确提取出感染主机、C&C服务器IP地址。

关键词 网络安全,僵尸网络,域名生成算法,域名变换

中图法分类号 TP393 **文献标识码** A

Malware Domains Detection by Monitoring Group Activities

ZHANG Yong-bin LU Yin ZHANG Yan-ning

(School of Computer Science, Northwestern Polytechnical University, Xi'an 710129, China)

Abstract At present, many botnets adopt Domain Flux techniques to avoid the block of domain blacklists. A new technique was proposed to detect malicious domain by analyzing group-behavior of compromised hosts on DNS queries. The method clusters new domains and Non-Existent domains queried by hosts in each epoch, groups these hosts by new domain names, and identifies that if the hosts within the same set have group activities when querying Non-Existent domains, to detect compromised hosts and IP addresses of C&C servers. The monitoring results for an ISP DNS show that compromised hosts and IP addresses of C&C servers are detected accurately.

Keywords Network security, Botnet, Domain name generation algorithms(DGA), Domain flux

1 概述

域名解析服务(DNS)将抽象的IP地址映射为易于记忆的域名,使互联网用户更加方便地访问各种网络资源,是互联网体系结构中重要的基础服务之一。DNS服务自身缺少恶意行为检测能力,因此常常被恶意程序利用,例如:僵尸主机通过DNS服务器解析相关域名,以便与C&C服务器建立连接,获取控制指令。为封堵这些恶意流量,域名黑名单被广泛使用,通过黑名单可有效过滤这些非法的域名请求。为对抗域名黑名单的封堵,目前Bot程序广泛采用了Domain Flux技术,这一技术通过特定的域名产生算法(Domain Generation Algorithms, DGA)定期生成大量新域名进行请求。每个周期生成的域名不同,并且数量巨大,有效地干扰了黑名单的检测和维护,如Conficker[1]、Kraken[2]、Torpig[3]等。以Conficker为例,Conficker.C以24小时为周期,采用网络时间作为域名产生种子,保证所有感染主机每个周期生成相同的域名,Conficker一个周期内生成长达5万条的随机域名列表。因此,为了防范僵尸网络的攻击行为,DGA生成域名的检测与封堵成为网络安全研究的重要课题。

本文以网络中主机的DNS请求为数据,对网络中主机请求的失效域名及新域名进行聚类,将主机划分为多个请求组,通过分析组内主机在域名请求行为上是否具有组行为特征,对采用DGA算法的Botnet进行检测,以便提取出感染主机集合、C&C服务器使用的IP地址集合。

2 相关研究及论文工作

2.1 相关研究

DGA算法在生成域名时无需考虑便于理解和记忆的问题,并且为了避免在新域名注册时发生冲突,DGA算法生成的恶意域名往往是一些字母、数字的随机组合,与正常域名在字符概率分布上有着显著不同。文献[4]针对DGA生成域名的文法统计规律特点,采用机器学习方法对程序生成域名进行识别,并对比域名的K-L距离、编辑距离、Jaccard系数分别作为特征向量的识别效果。文献[5]采用了文献[4]类似思想,通过采用全变差距离作为特征向量,通过朴素贝叶斯分类算法对算法产生域名进行识别。文献[6]通过对解析失败的域名请求进行分析,建立请求主机与解析失败域名之间的关系图,通过图分解的方法将DNS关系图分解为子图并进行研究,发现不同的子图结构往往代表不同的恶意行为。文献[7]通过对解析成功的域名与失败的域名进行时间相关分析、信息熵分析,检测网络中存在的域名变换行为,并提取出C&C服务器对应的IP地址。文献[8]对顶级域名服务器进行监测

到稿日期:2012-10-12 返修日期:2013-01-28 本文受国家自然科学基金(60903126,60872145)资助。

张永斌(1976—),男,博士,主要研究方向为信息安全,E-mail:zhangybmail@163.com。

分析，对比了合法域名与恶意域名的请求行为的不同。文献[9-11]利用机器学习的方法，分别提出了3种不同的域名信誉系统来对恶意域名进行检测，其中Notos、Exposure主要通过旁路报文捕获的方式对网络中主机域名请求流量或DNS服务器流量进行监测，Kopis主要是对顶级域名服务器、授权服务器进行监测，与Notos、Exposure系统相比，Kopis可以从全球视角对域名的请求情况进行监测与分析。

2.2 论文工作

Bot程序一般以24小时为一个周期，每个周期通过特定的DGA算法生成大量的新域名，以提高整个感染网络的鲁棒性和抗封堵能力。出于经济成本的考虑，僵尸网络的控制者不可能注册全部生成域名，而是从生成的域名中抽取一个子集完成注册。通过事先注册一个或多个域名，控制者便可实现对整个网络的控制。对于Bot程序，为实现与C&C服务器建立连接，必须对生成域名进行解析，直至获取C&C服务器的IP地址，由于注册的域名数量有限，导致感染主机会请求大量新域名，并存在一定数量解析失败的域名请求行为。当网络中存在多台感染相同Bot程序的主机时，这些感染主机与正常主机相比，在DNS请求行为方面具有以下两个明显的组行为特征：

1)DGA算法必须保证每个感染主机在每个周期内生成相同的域名集合，由于生成域名集合中注册的域名有限，当网络中有多台感染主机时，将导致感染主机会请求一组特定的失效域名集合。

2)DGA算法每个周期生成的域名往往不同，导致感染主机在每个周期会请求大量新域名，且这些域名只有感染主机才会请求。由于Botnet控制者所拥有的IP资源十分有限，感染主机请求域名的解析结果往往指向相同的IP地址，因此，可通过域名解析返回的IP地址将感染主机汇聚在一起。

通过对主机请求的失效域名及新域名进行聚类分析，将请求同一组新域名的主机集合作为检测对象，通过分析同一集合内主机域名请求行为是否具有组特性，对采用DGA技术的Botnet进行检测，以提取出感染主机集合、C&C服务器使用的IP地址集合。论文所采用的算法主要从感染主机的域名请求行为特征出发，与文献[7,8]相比无需太多的先验知识，与文献[9,10]相比复杂度低，同时可以快速提取出C&C服务器地址集合，以便建立IP黑名单对恶意流量进行封堵。

3 算法设计与实现

整个检测算法分为：数据预处理、失效域名聚类分析、新域名聚类分析、恶意域名提取4个处理过程。其中数据预处理过程主要是判断一个解析成功的域名是否是新域名，并将网络中主机请求的新域名及失效域名信息进行保存，以便后续分析。失效域名聚类分析过程主要是通过请求失效域名的主机IP地址信息对失效域名进行聚类分析，提取出可疑失效域名集合、潜在感染主机集合。新域名聚类分析过程主要是通过新域名解析返回的IP地址对新域名进行聚类分析，利用聚类结果，将请求主机划分为多个请求组。恶意域名提取过程主要是通过失效域名聚类结果，对请求每个新域名集合的主机组进行分析，判断组内主机在域名请求行为上是否具有组行为特征，提取出最终的恶意域名、感染主机、C&C服务器IP地址集合，并对分析结果进行评估。

3.1 数据预处理

为实现新域名的判断，系统工作过程分为学习与检测两个阶段。在每个工作阶段，系统首先通过域名白名单对可信、合法的域名请求进行过滤，降低后续的处理数据量。在学习阶段，系统对网络中所有主机成功请求过的域名进行收集、保存，通过一段时间的学习后，形成一个相对完善的域名数据库，建立检测基线。由于互联网资源访问服从幂律分布，经过一段时间学习后，网络中每天出现的新域名数量相对有限，产生新域名请求的正常主机数量也相对较少。在检测阶段，系统通过已建立的域名数据库，对解析成功的域名进行判断，如果不在域名数据库中，则认为主机请求了一个新域名，将请求信息进行保存，在该阶段系统同时对网络中主机请求的失效域名进行记录，以便进一步分析。

3.2 失效域名聚类分析

系统主要对运营商的DNS服务器进行监测，由于Bot程序具有很强的传染能力[12,13]，在ISP网络内往往存在几十台甚至上百台感染主机，感染主机数量越多，感染主机共同请求特定失效域名集合的组行为特征越明显。目前，NAT技术、代理技术在互联网建设中广泛使用，一个主机IP地址的域名请求行为可能是多个主机的混合行为，因此，无法直接通过主机请求的失效域名对主机进行聚类，将主机划分为多个请求组。系统采取对失效域名的聚类分析，实现请求主机的划分，以解决上述问题。在每个检测周期内(系统默认周期为一天)，系统通过IP地址对每个主机进行标识，将每个检测周期内主机请求的失效域名集合记为：$Q_F=\{d_{F1},d_{F2},\cdots,d_{Fn}\}$，$QIP_i$为请求失效域名$d_{Fi}$的主机集合。在每个检测周期结束时，系统通过层次聚类中全连接方法，对所有请求主机数量$|QIP_i|$大于阈值λ的失效域名进行聚类分析，通过请求失效域名主机集合间的Jaccard系数来定义失效域名间的距离，即：

$$dist(d_{Fi},d_{Fj})=1-\frac{|QIP_i\cap QIP_j|}{|QIP_i\cup QIP_j|}$$

通过聚类分析，系统将请求主机相近的失效域名划分到一组，同时在此过程中也将请求主机划分为多个请求组。由于感染主机请求的失效域名较多，系统只选取聚类结果中域名数量大于阈值θ的类作为可疑域名集合，进行下一步分析，并将其记为：$FC_1,FC_2,\cdots,FC_m$，相应请求主机集合Hf_k作为潜在的感染主机集合，$Hf_k=\bigcup_{i=1}^{l}QIP_i,d_i\in FC_k$。经试验，$\lambda\geqslant 10,\theta\geqslant 10$。聚类阈值选取0.3时，感染主机可有效划分到同一组中。

3.3 新域名聚类分析

由于感染主机具有请求新域名的行为特征，系统通过数据预处理步骤，将每个检测周期内主机成功解析的新域名集合记为$Q=\{d_1,d_2,\cdots,d_n\}$，RIP_i为域名d_i解析返回的所有IP地址集合。尽管感染主机通常随机访问域名生成列表中的域名，致使感染主机成功连接C&C服务器所使用的域名不一定相同，但是这些新生域名往往都指向相同的IP地址。定义域名间关系图G，G中节点i为域名d_i，G中任意两个节点d_i,d_j，若$RIP_i\cap RIP_j\neq\Phi$，则认为两个节点间存在边，否则不存在边。G中任意一个连通子图G_k称为域名关联集合C_k，C_k中所有域名对应的IP地址集合记为$RIPc_k$，请求主机集合记为Hc_k(Hc_k中任意主机至少请求过C_k中一个域名)。通过连通子图特性可知，对于C_k中任意一个域名d_i，其满足

如下关系：$\forall d_i \in C_k$，则 $\exists d_j \in C_k, i \neq j, RIP_i \cap RIP_j \neq \Phi$。通过对 G 的连通子图进行分析，可有效地将网络中请求新域名的主机划分为不同的请求组，以便进一步分析每个请求组内主机间是否具有一致的组行为。为得到 G 中所有连通子图及相应的请求主机组，可通过由下至上的层次聚类方法对 Q 中域名进行聚类分析，聚类使用的距离函数定义为：

$$dist(C_i, C_j) = \begin{cases} 0, & RIPc_i \cap RIPc_j \neq \Phi \\ +\infty, & RIPc_i \cap RIPc_j = \Phi \end{cases}$$

3.4 恶意域名提取

对于感染同一种 Bot 程序的主机，每个周期内 DGA 算法生成的域名列表完全相同，同时由于 IP 资源的限制，域名列表中已注册的域名往往指向相同的 IP 地址，因此，对于任意域名关联集合 C_i，如果请求主机组 Hc_i 中大量主机具有请求同一组失效域名 FC_j 的行为，则 C_i 为 Botnet 使用的域名集合可能性较高。同样，对于任意失效域名集合 FC_j，如果请求主机 Hf_i 中大量主机请求了相同的新域名组 C_i，则说明 Hf_k 中主机在域名请求行为上具有明显的组特性，也具有很高的可疑性，因此，定义评估指标 $Sc_{ij} = \frac{|Hc_i \cap Hf_j|}{|Hc_i|}$，$Cc_{ij} = \frac{|Hc_i \cap Hf_j|}{|Hf_i|}$，其中 Sc_{ij} 称为可疑度指标，主要衡量 Hc_i 中主机在请求失效域名行为上是否具有组行为特征，通过该指标可以有效排除合法的新域名请求行为及已不在活动的 Botnet。Cc_{ij} 称为一致性指标，与 Sc_{ij} 类似，主要衡量 FC_j 中主机在请求新域名行为上是否具有组行为特征，通过该指标可以有效排除正常 P2P 应用产生的域名解析失败行为。在实际检测过程中，当 $Sc_{ij} \geqslant \delta$ 且 $Cc_{ij} \geqslant \gamma$ 时，则认为域名关联集合 C_i 为 Botnet 当前使用的域名集合，对应 Hc_i 为感染主机集合，$RIPc_i$ 为 C&C 服务器 IP 地址集合。经实际测试，选取 $\delta \geqslant 0.75$，$\gamma \geqslant 0.5$ 具有很好的甄别效果。

4 实验验证

实验数据主要源于某地市 ISP 的 DNS 服务器集群，在上网高峰期时段，该 DNS 服务器集群接收 DNS 请求平均 1.2 万次/秒，服务近 20 万用户。系统采集了 45 天的域名请求信息，并建立域名基线数据库，其中包含 869 万个域名、1900 多万条域名与 IP 地址对应信息。基线建立后，选取了 5 天的数据进行分析。

4.1 一天数据分析结果

由于实验分析数据过多，在文中选取了第 5 天的数据，对失效域名聚类条件即聚类阈值为 0.3、请求主机数量阈值 $\lambda \geqslant 10$ 时的情况进行讨论。

4.1.1 失效域名聚类的结果

当天请求失效域名的 IP 地址数量为 64579 个，失效域名的数量为 145593 个，其中大量域名仅有一个主机请求（CDF 曲线参见图 1），请求主机数量超过阈值 λ 的域名数量仅有 1787 个。通过聚类分析后，得到 1186 组域名集合，其中域名集合至少包含 2 个域名的集合仅有 87 组，通过谷歌查询，这 87 组中确认为 P2P 应用相关的域名有 58 组，恶意域名有 8 组。对于 8 组恶意域名，其中 5 组域名集合所包含域名数量均小于 5 个，通过查询到的恶意软件分析报告可知：属于恶意软件绑定多个域名情况，如：x-77. cn、x-66. cn、www. fdsa432fsat4s2os. com、www. fdsa432fsatf32os. com 等。剩余 3 组属于 DGA 算法生成域名，包含的域名数量分别为：32、47、88 个，具体域名参见表 1。

表 1 DGA 生成域名

Set-1	Set-2	Set-3
1. nsvhn987. com	1. nslook001. com	rcuedqxj. com
2. nsvhn987. com	2. nslook001. com	rrxgi. cc
79. nsvhn987. com	……	rvaeigmcni. cc
……	77. nslook001. com	nbkimso. net
1. ns2275ab. com	76. nslook001. com	qosgvrfiro. cc
2. ns2275ab. com	……	qozajttafml. com
56. ns2275ab. com	85. nslook001. com	slkaqrwx. cc
79. nsvhn987. com	……	rywlzg. net
……		……

4.1.2 新域名聚类的结果

当天请求新域名的 IP 地址数量为 150981，新域名的数量为 119427，其中当天新域名数量为 25877。从域名请求主机数量上来看，对于大量域名只有 1 个 IP 请求（见图 1），经聚类分析后，得到 34558 组域名集合，其中 28463 组只有一个 IP 访问。

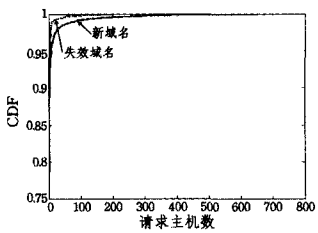

图 1 域名请求 CDF 曲线

4.1.3 恶意域名提取结果

选取 Hc_k、θ、Sc_{ij}、Cc_{ij} 的阈值分别为 5、5、0.7、0.0 时，符合条件的新域名有 6 组，其中 $Cc_{ij} \geqslant 0.1$ 的只有 2 组，符合条件的失效域名集合有 3 组，其中 2 组为 P2P 应用站点，1 组为表 1 中的 Set-3，具体 Sc_{ij}、Cc_{ij} 及请求主机数量参见表 2。

表 2 SC、CC 计算结果

失效域名类型	SC	CC	请求新域名主机数	请求失效域名的主机数
DGA	0.994	0.8228	369	446
DGA	0.977	0.8497	388	446
P2P	0.786	0.0095	14	1157
P2P	0.7	0.0019	10	3568
P2P	0.857	0.0016	7	3568
P2P	0.833	0.0014	6	3568

通过表 2，可以看到 Cc_{ij} 较小的组主要是 P2P 站点，分析造成的主要原因是：很多 P2P 资源的种子文件中包含了一些已不可用的 Tracker 服务器信息，如：denis. stalker. h3q. com、tracker. publicbt. org，导致请求主机产生域名失效行为，通过失效域名聚类分析将这些主机划分到同一组，由于请求主机数量较大，其中少部分主机请求了相同的新域名。

对于 3 组 DGA 生成域名，Set-3 被成功检测出来，可以看到其 Sc_{ij}，Cc_{ij} 的值均很高，通过对请求主机集合进行分析，发现它们基本为同一组主机，即：这 2 组新域名集合是由同一 Botnet 产生的，经确认为 Conficker 生成的域名当天请求 IP 多达 388 个，使用的域名集合、C&C 服务器地址参见表 3。另外两组 DGA 生成域名没有被检测出来，分析域名库中的域名，在整个监测期间，相关域名从未解析成功，即：无法通过这些域名与 C&C 服务器建立连接。这种情况不是本文关心

（下转第 185 页）

加权距离。经验证，NLOF 算法能够有效提高离群点检测精度，降低计算复杂度。但是在 NLOF 算法中，参数 k 的作用重大，直接影响到邻近点的邻域查询范围。因此，下一步将研究参数与运行时间、运行结果之间的关系，找出自动提供合理的各参数值的方法。

参 考 文 献

[1] Hawkins D. Identification of Outliers [M]. Londen: Chapman and Hall, 1980: 188

[2] Han Sang-jun, Cho S-B, et al. Evolutionary Neural Networks for Anomaly Detection Based on the Behavior of a Program [J]. IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics, 2006, 36(3): 559-570

[3] Ramaswamy S, Rastogi R, Shim K. Efficient algorithms for mining outliers from large data sets[J]. ACM Sigmoid Record, 2000, 29(2): 427-438

[4] Hung Wen-liang, Yang Min-shen. An Omission Approach for Detecting Outliers in Fuzzy Regression Models [J]. Fuzzy Sets and Systems, 2006, 157(23): 3109-3122

[5] Liu Xiao-hui, Cheng Gong-xian, Wu J X. Analyzing Outliers Cautiously[J]. IEEE Transactions on Knowledge and Data Engineering, 2002, 14(2): 432-437

[6] Breunig M, Kriegel H P, Ng R, et al. LOF: Identifying Density-based Local Outliers, 2000[C]// Proc. of the ACM SIGMOD International Conference on Management of Data. [s. l.]: ACM press, 2000: 93-104

[7] Tang J, Chen Z, Fu A, et al. Enhancing effectiveness of outlier detections for low-density patterns, 2002[C]// Proceeding of Advances in Knowledge Discovery and Data Mining 6th Pacific Asia Conference, Lecture Notes in Computer Science. Taipei, China, 2002: 535-548

[8] Ni Wei-wei, Chen Geng, Lu Jie-ping, et al. Local Entropy Based Weighted Subspace Outlier Mining Algorithm[J]. Journal of Computer Research Development, 2008, 45(7): 1189-1194

[9] Papadimitirou S, Kitagawa H, Gibbons P B, et al. LOCI: Fast outlier detection using the local correlation integral [C]// Proc of the 19th Int Conf on Data Engineering. Los Alamitos: IEEE Computer Society, 2003: 315-326

[10] 薛安荣，鞠时光，何伟华，等. 局部离群点挖掘算法研究[J]. 计算机学报，2007，30(8)：1455-1463

[11] 胡彩平，秦小麟. 一种基于密度的局部离群点检测算法 DLOF [J]. 计算机研究与发展，2010，47(12)：2110-2116

[12] 张净，孙志挥，等. 基于信息论的高维海量数据离群点挖掘[J]. 计算机科学，2011，38(7)：148-161

(上接第 148 页)

重点，本文重点检测的是正在活动的恶意域名。

表 3 恶意域名及 C&C 的 IP 地址

成功域名	C&C 地址
jalkd. cn	221. 8. 69. 25
izgj. cn	
ywhweot. cn	
yelicsefau. org	143. 215. 130. 33
ycbptbn. org	143. 215. 143. 11
xvnfoedv. org	149. 20. 56. 32
xuhsjusol. org	149. 20. 56. 33
	149. 20. 56. 34

4.2 最终检测结果

当失效域名聚类阈值为 0. 3、$\lambda \geqslant 10$，$\theta \geqslant 10$，Sc_{ij}，Cc_{ij} 的阈值分别 0. 75，0. 5 时，对 5 天的数据进行分析，提取出 3 组 C&C 服务器地址，其中两组地址为表 3 中的 C&C 服务器地址，这两组地址连续 5 天都出现，但每天对应的域名不同，请求 IP 数量主机最多时达 467 个不同 IP 地址。另外 1 组(域名为 roish. com、IP 地址为：74. 117. 116. 65)只出现了 1 天，同时当天请求主机与另外两组的请求主机基本相同，并且域名对应的网站是合法网站，判断被提取的出原因是：DGA 算法生成域名与已有域名发生冲突。

结束语 本文通过研究主机请求域名的行为特征，对采用 DGA 技术的 Botnet 进行检测，通过实际环境的验证，可以有效地检测出感染主机集合及 C&C 服务器使用的 IP 地址集合。未来研究中，将结合 DGA 生成域名字符构成特征，对失效域名集合、C&C 服务器 IP 地址进行进一步的检测。

参 考 文 献

[1] Leder W. Know Your Enemy: Containing Conficker [R]. The Honeynet Project & Research Alliance, University of Bonn, Germany, 2009

[2] Royal P. On the kraken and bobax botnets[R/OL]. http://www.damballa. com/downloads/r_pubs/Kraken_Response. pdf, 2009

[3] Stone-Gross B, Cova M, Vigna G. Your Botnet is My Botnet: Analysis of A Botnet Takeover [C]// ACM Conference on Computer and Communications Security(CCS). 2009: 635-647

[4] Yadav S, Reddy A, Ranjan S. Detecting Algorithmically Generated Malicious Domain Names [A]// 10th Annual ACM Conference on Internet Measurement [C]. New York, USA, 2010: 48-61

[5] Stalmans E, Irwin B. A Framework for DNS Based Detection and Mitigation of Malware Infections on a Network [A]// Information Security South Africa(ISSA)[C]. 2011: 76-83

[6] Jiang N, Zhang Z. Identifying Suspicious Activities through DNS Failure Graph Analysis [A]// Network Protocols(ICNP), the 18th IEEE International Conference [C]. 2010: 144-153

[7] Yadav S, Reddy A N. Winning with DNS Failures: Strategies for Faster Botnet Detection [A]// 7th International ICST Conference on Security and Privacy in Communication Networks [C]. 2011: 133-145

[8] Hao S, Feamster N, Pandrangi. An Internet Wide View into DNS Lookup Patterns[R/OL]. http://labs. verisigninc. com/projects/malicious-domain-names. html, 2010

[9] Antonakakis M, Perdisci R, Dagon D, et al. Building A Dynamic Reputation System for DNS [A]// the Proceedings of 19th USENIX Security Symposium (USENIX Security' 10) [C]. 2010: 273-289

[10] Antonakakis M, Lee R, Dagon D. Detecting Malware Domains at the Upper DNS Hierarchy [A]// the Proceedings of 20th USENIX Security Symposium(USENIX Security '11)[C]. 2011: 23-46

[11] Bilge L, Kirda E, Kruegel C, et al. Exposure: Finding Malicious Domains using Passive DNS Analysis [A]// Proceedings of NDSS [C]. 2011: 1-17

[12] 黄彪，成淑萍，欧阳晨星，等. 无尺度网络下具有双因素的僵尸网络传播模型[J]. 计算机科学，2012，39(10)：78-81

[13] 冯丽萍，韩琦，王鸿斌. 具有变化感染率的僵尸网络传播模型[J]. 计算机科学，2012，39(11)：51-53