基于行为与域名查询关联的僵尸网络聚类联动监测 *

袁春阳[1], 李青山[2], 王永建[1]
(1. 国家计算机网络应急技术处理协调中心, 北京 100087; 2. 北京大学 网络与软件安全保障教育部重点室, 北京 100087)

摘 要: 为了解决基于特征的监测只能监测到已知的 botnet,且监测方法很大程度依赖于 botnet 所采用的协议和结构的问题,提出基于行为与域名查询关联的 botnet 监测方法。利用相同僵尸网络中的各个僵尸活动相互之间具有时间、空间的行为相关性和相似性特点,对 botnet 的行为流和域名查询流进行聚类,给出一种聚类联动的监测模型。通过采集、分析部署在某市营运机房 DNS 缓存服务器上的实验系统反馈数据,证明该聚类联动监测模型不仅能够监测未知 botnet,而且监测过程与 botnet 采用的协议结构无关,具有较好的监测效率。

关键词: 行为关联; 域名分析; 僵尸网络; 聚类; 联动监测
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)03-1084-04
doi:10.3969/j.issn.1001-3695.2012.03.078

Linkage monitoring of cluster for botnet based on relevance of behavior and domain inquiry

YUAN Chun-yang[1], LI Qing-shan[2], WANG Yong-jian[1]
(1. *National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing* 100087, *China*; 2. *Key Laboratory of Network & Software Security Assurance of Ministry of Education, Peking University, Beijing* 100087, *China*)

Abstract: Feature-based monitoring can only monitor known botnet, and monitoring methods depend heavily on the structure and the protocol of botnet used. This paper proposed botnet monitoring methods based on behavior associated with the domain name query to solve the problems. It clustered the behavior and domain name query flow of botnet utilizing related and similar characteristics exist in activities among the various bots on time and space. Proposed a linkage monitoring model on clustering. Through the collection and analysis the feedback data of DNS cache server on the test system deployed operating room in the city, it is proved that the linkage monitoring model on clustering can not only monitor the unknown botnet, but also monitoring process independent of the protocol and structure used. It has a good monitoring efficiency.

Key words: behavior relevance; domain analysis; botnet; cluster; linkage monitoring

0 引言

僵尸网络(botnet)是黑客利用僵尸程序控制大量主机(即僵尸主机)所形成的被控主机群。利用僵尸网络,攻击者可实施信息窃取、垃圾邮件、网络仿冒、拒绝服务攻击等各种恶意活动。僵尸网络已成为当前互联网的主要安全威胁之一。传统的基于特征的监测方法虽然能进行较为精确的监测,满足监测实时性要求[13],但是这种方法只关注 botnet 表面特性,不能很好反映 botnet 的本质,且必须使用先验知识进行匹配[4],因此只能监测已知的 botnet。若 botnet 改变其使用的协议规则形成一种新的结构,这些监测方法则会失效。

现有的僵尸网络大部分都采用 IRC 协议、P2P 协议,或者 HTTP 协议构成[58],无论是采取何种协议结构,bot 通过域名系统查询相应的 C&C 僵尸服务器地址并连接通信,是 botnet 的核心,也是最基本的行为。基于域名查询的监测方法正是针对僵尸网络的这种行为本质提出的,运用这种方法进行监测可以突破 botnet 所采用的协议与结构的限制,具有较好的可扩展性。

Dagon 等人[9]提出利用侦查在极短时间内存在频繁的动态 DNS 请求的主机来识别 botnet 的 C&C 服务器。这和 Kristoff[10]在 2004 年提出的技术具有相似性,但这两种技术都存在一个共同的弱点,即可以利用伪造的 DNS 查询欺骗并入侵监测系统。此外,文献[11]指出,针对那些使用了短时间生命周期(short time-to-live)连接的合法的、流行的域名系统,运用这种技术将会对这些域名系统产生错误的类别划分,从而导致误判。

Schonewhile 等人[12]在 2006 年提出将域名服务器(DNS)作为一个入侵监测系统监测僵尸程序,主要通过采集和分析 DNS 数据来完成。分析过程包括已知的恶意域名查询、被感染主机的查询、异常查询、域名监测时间差、不常用的查询等。但这种方法不能进行实时监测。Ramachandran 等人[13]尝试使用启发式教育方法被动分析域名黑名单(DNSBL)的查询流量识别僵尸网络,结果表明该技术对早期僵尸程序监测很有帮

收稿日期: 2011-08-17; **修回日期**: 2011-09-27 **基金项目**: 国家"242"信息安全计划项目(2010A009)

作者简介: 袁春阳(1979-),男,高级工程师,博士,主要研究方向为网络与信息安全(jiren191@sina.com);李青山(1977-),男,硕士研究生,主要研究方向为网络与信息安全;王永建(1977-),男,副研究员,博士(后),主要研究方向为网络与信息安全.

助,而且能够进行实时监测,但在误报率方面需要改进。

基于此,研究高效的域名安全监测系统来有效监测僵尸网络成为一个亟待解决的问题。

1　问题解决思路

由于僵尸网络中的僵尸程序是受到僵尸服务器(C&C)的控制命令所控制,而僵尸主机对 C&C 服务器命令的响应又是事先编程决定的,所以相同僵尸网络中的各个僵尸相互之间具有时间、空间的行为相关性和相似性。例如,在相同时间段对大量其他主机进行非法扫描获取漏洞、向其他主机群发邮件、在某个时间段里同时向 DNS 请求某个服务器物理地址以便能够和该服务器通信并执行命令等。反之,正常网络行为则基本不会体现出相关和相似。

为了克服基于特征的监测模型只能监测已知 botnet,且和 botnet 所采用的协议和结构密切相关的局限性,提高 DNS 监测的精准性和高效性,本文提出一种聚类关联数据自适应的动态聚类技术,以实现 botnet 的行为流和域名查询流的高效联动聚类,并利用聚类的结果快速定位僵尸网络。

2　僵尸网络的联动监测模型

本文提出一种僵尸网络的联动监测模型(behavior-domain),模型从网络流量为出发点,对僵尸程序(bot)的各种恶意行为以及对 DNS 请求、应答查询流量进行联动监测,生成相关日志。引入 max-min 均值聚类算法对监测日志进行聚类,经过关联分析进行综合评价,从而识别僵尸网络。

2.1　Behavior-Domain 监测模型的系统结构

Behavior-Domain 监测模型主要由行为监视模块,域名请求、查询监视模块,行为和域名请求、查询聚类及关联分析模块构成。模型的系统结构如图 1 所示。

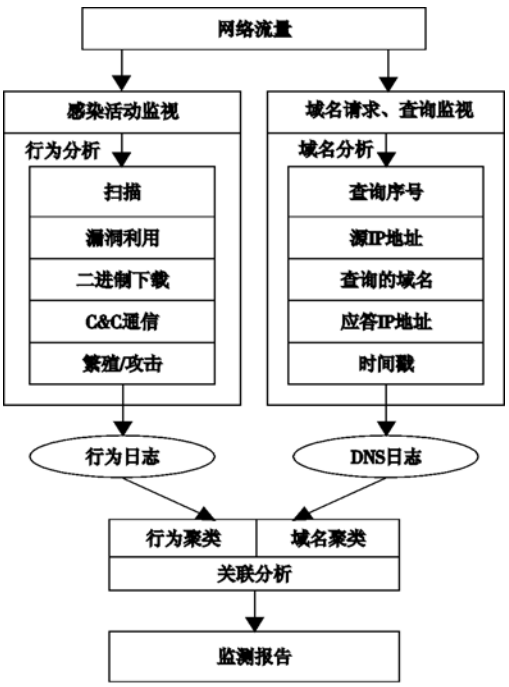

图1　Behavior-Domain监测模型系统结构

系统的运行过程如下:

a)由于处于同一通信信道的不同 bot 对 botnet 控制命令的行为响应及对 DNS 请求、查询响应有着极为相似的时间相关性,本文将行为监视模块和域名请求、查询监视模块部署在网络流量的出入口处,对出入口流量进行实时监测和采集。(a)行为监测模块及时捕获并解析 botnet 命令控制信道内诸如扫描、网络漏洞利用、二进制下载、C&C 通信、繁殖/攻击等行为流量,将结果存入行为日志中;(b)域名请求、查询监测模块监测域名请求、查询响应数据包,并将解析得到的相关记录存入指定的 DNS 日志文件中。

b)聚类模块是监测模型的核心模块。它负责定时到指定的 Log 日志中提取相应的信息,利用 max-min 均值聚类算法分别对提取的两类网络信息日志中的数据进行聚类,聚类的结果导入关联分析模块便于进行关联分析。

c)关联分析模块首先进行可疑度的计算,并将计算结果与事先给定的阈值 θ 比较,以便判断目标是否是僵尸主机。其次计算相似度,判定同一个流类簇集合中的两台僵尸主机是否属于同一个僵尸网络。最终结果形成监测报告输出。

2.2　行为及域名请求、查询监视

1)行为监视模块　通过分析被监视网络出、入数据流及数据包的内容,监测网内主机执行的恶意行为,并形成 Log 日志。由于 botnet 控制者通常发起漏洞扫描、漏洞利用/缓冲区溢出、二进制下载、C&C 异常通信以及繁殖/攻击等恶意行为,因此监测模块主要关注这五类恶意行为。

2)域名请求、查询监视模块　通过分析各个主机对域名系统发出的请求、查询数据包的内容,形成请求、查询 Log 日志。日志中包含查询号、源 IP 地址、查询的域名、应答 IP 地址、时间戳等原始数据。

2.3　行为及域名请求、查询聚类算法

针对标准的 k-均值聚类算法存在计算复杂度高、运行时间长、可能收敛到局部最小,其 k 值必须事先确定,且算法对初始化中心敏感等缺点,提出一种利用最大最小距离找到中心点的 Max-min 均值聚类算法用于行为及域名请求、查询聚类。

定义 1　$S_n=(a_1,a_2,\cdots,a_n)$ 表示等待聚类的对象集合,初始聚类中心集合记做 C,C 初始为 φ。

Max-min 均值聚类算法思路如下:

a)随机选取一个对象 a_1 作为第一个聚类的中心,记做 $Z_1=a_1$。在集合 S 中找到距离 Z_1 最大的对象,假设为 a_2,则 $Z_1=a_2$,作为第二个聚类的中心。

b)对 S_n 中剩余的每个对象 a_i,计算 a_i 到 Z_1、Z_2 的距离。取两个距离中最小的距离,记做:

$$D_{ai}=\min\{|a_i-Z_1|,|a_i-Z_2|\},$$

S_n 中剩余对象的 D_{ai} 集合记做 $S_n\{D_{ai}\}$。

c)找到 $S_n\{D_{ai}\}$ 中的最大值 $\max S_n\{D_{ai}\}$,假定该最大值对应的对象是 a_i,判断其是否满足检验式 $\max S_n\{D_{ai}\}>1/2\times(|Z_1-Z_2|)$,若满足则取 a_i 为新的聚类中心,此时 $Z_3=a_2$。

d)对 S_n 中剩余的每个对象分别计算它们到每个聚类中心的距离,令 $D_{ai}=\min\{|a_i-Z_1|,|a_i-Z_2|,|a_i-Z_3|\}$,计算 $\max S_n\{D_{ai}\}$,若满足检验式

$$\max S_n\{D_{ai}\}>1/2\times\text{average}\{(|Z_1-Z_2|),(|Z_2-Z_3|)\}$$

则取最大值对应的对象 a_i 作为新的聚类中心。

e)重复步骤 d)直至找不到符合检验式条件的新的聚类中心。

Max-min 均值聚类算法不仅不用预先确定 K 值和初始的聚类中心,而且能避免两个聚类中心的点过于接近。

2.4　关联分析

单独通过行为聚类和域名查询聚类分析都不能准确定位

网络中的僵尸主机,将两者结合起来进行关联分析,则可以进一步判定目标主机是否属于同一个僵尸网络,从而有效解决以上问题。思路如下:

a)在行为聚类分析结果中选取具有恶意行为的主机 h,计算可疑度 $s(h)$。

b)比较可疑度 $s(h)$ 与给定的阈值 θ,若 $s(h)>\theta$,则可判定 h 是可疑僵尸主机,反之则判定为正常主机。

c)计算相似度 $\mathrm{sim}\,A(h_i,h_j)$,若 $\mathrm{sim}\,A(h_i,h_j)\geqslant 1$ 且 h_i 与 h_j 属于同一个域名查询流类簇集合,则可判定它们属于同一个僵尸网络。

给出可疑度 $s(h)$ 以及相似度 $\mathrm{sim}\,A(h_i,h_j)$ 的定如下:

定义 2　假定有恶意行为的主机集合为 H,H 由行为聚类分析结果给出,集合中的每台主机 $h\in H$,并且 $A^{(h)}=\{A_i\}_{i=1,\cdots,m_h}$ 是包含主机 h 的 m_h 个行为类簇集合,$D^{(h)}=\{D_i\}_{i=1,\cdots,n_h}$ 是包含主机 h 发出的 n_h 个查询服务器域名的类簇集合。则可疑度记为

$$s(h)=\sum_{\substack{i,j\\ j>i\\ t(A_i)\neq t(A_j)}} w(A_i)w(A_i)\frac{|A_i\cap A_j|}{|A_i\cup A_j|}+\sum_{i,k}w(A_i)\frac{|A_i\cap D_j|}{|A_i\cup D_j|}\qquad(1)$$

其中:$A_i,A_j\in A^{(h)}$,$D_k\in D^{(h)}$,$t(A_i)$ 为行为类簇 A_i 的类型,如扫描、漏洞利用、二进制下载以及拒绝服务攻击等行为类型。$w(A_i)$ 为不同 A_i 的权重,$w(A_i)\geqslant 1$,且不同 A_i 权重各不相同,权重值取决于该类簇表示的恶意行为出现的概率。概率越大,则与之对应的 $w(A_i)$ 越大。

式(1)的前半部分表示某个主机同时执行 $m\geqslant 0$ 个恶意行为的分值。可以看出,$m=0$ 表示没有恶意行为,该部分值为 0;$m\geqslant 1$ 则表示出现了 m 种类型的恶意行为。式(1)的后半部分则表示域名查询类簇中出现恶意行为 A_i 的分布状况。当 $s(h)\geqslant\theta$ 则说明主机进行了恶意行为或异常域名查询。

例如,假设 h 同时进行了对外扫描和漏洞探测两种行为,A_1、A_2 分别代表 h 所在的对外扫描类簇和漏洞探测类簇中所有主机的集合,若 A_1、A_2 重叠部分越多,即 $A_1\cap A_2$ 的值越大,相应 $s(h)$ 的值也越大。同理,若 h 所在的恶意行为类簇和域名查询类簇重叠部分越多,则说明相应的主机不仅执行相同的恶意行为,而且具有相同的通信模式,则判定这些主机是同一僵尸网络中的僵尸主机的可能性也就相应增大。

定义 3　假定已通过行为聚类监测判定为可疑的主机簇为 $B(B\subseteq H)$,H 为有恶意行为的主机集合,$A^{(B)}=\{A_i\}_{i=1,\cdots,m_B}$ 是至少包含一个可疑主机 $h\in B$ 的行为类簇,$C^{(B)}=\{C_i\}_{i=1,\cdots,n_B}$ 是至少包含一个可疑主机 $h\in B$ 的查询类簇。将行为类簇、查询类簇并集形成:

$$k^{(B)}=A^{(B)}\cup C^{(B)}=\{K_i^{(B)}\}\qquad i=l,\cdots,m_B+n_B$$

每一个 $h\in B$ 可以被描述为二进制向量 $b(h)\in(0,1)^{|K^{(B)}|}$,若 $h\in K_i^{(B)}$,则第 i 个元素 $b_i=1$;否则 $b_i=0$。介于这种描述,定义可疑主机 h_i、h_j 的相似度 $\mathrm{sim}\,A(h_i,h_j)$:

$$\mathrm{sim}\,A(h_i,h_j)=\sum_{k=1}^{m_B}I(b_k^i=b_k^j)+I\Big(\sum_{k=m_B+1}^{m_B+n_B}I(b_k^i=b_k^j)\geqslant 1\Big)\qquad(2)$$

为便于描述,令 $b^{(i)}=b(h_i)$,$b^{(j)}=b(h_j)$,$I(X)$ 是判定函数,当布尔参数 X 为真时,函数值为 1;否则函数值为 0。式(2)说明,如果两台主机 h_i 和 h_j 出现在同一个行为类簇中,并且至少出现在一个公共的查询类簇中,它们将聚类在一起,从而可判定主机 h_i 和 h_j 处于同一个僵尸网络,如图 2 所示。

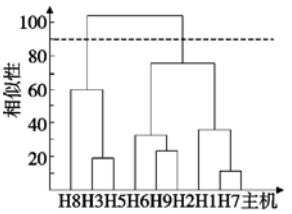

图2　聚类过程描述

2.5　僵尸服务器的定位

本文根据行为和域名查询聚类初步判定了可能的僵尸主机类簇之后,由于该类簇中的主机发出的域名查询能形成一个组群行为,通过监测域名流的组群行为的独特特征,可以区分僵尸网络的域名查询和正常合法的域名查询,从而进一步确定僵尸网络中的僵尸服务器。具体方法如下:

a)初始化。

$t-1$ 至 t 时间内 DNS 的查询记录 Q_t;DNS 查询记录的存储数组 A_t;Q_t 的域名答复 DN_k。

b)插入过程。

```
if   DN_k ∉ A
     insert(DN_k, A)
     IP_k, IPList_k = IP address of Q_t, IPList_k o f DN
     insert(IP_k, IPList_k)
      else   if   IP_k ∉ IPList_k
                  cnt_k + +
                  insert(IP_k, IPList_k)
return
```

c)删除过程。

```
int k = 1
while(k < n)
W,T = WhiteList, size threshold
if (DN_k ∈ W) or (DN_k⇒cnt < A)
   delete(DN_k, A_t)
   k + +
return
```

d)监测过程。

```
int k = 1
while(k < n)
if (At1⇒DN_k) = (A_t⇒DN_k)
   sim_DNS(At_1⇒IPList_k, At_2⇒IPList_k)
   s = computed sim_DNS
   if
   DN_k is botnet name
   else if s = -1
   insert (BL, DN_K)
   BL = Black List
   else insert (W, DN_k)
return
```

e)结果分析。

相关性 $\mathrm{sim}_{\mathrm{DNS}}$ 判定式如下:

$$\mathrm{sim}_{\mathrm{DN}S}(h)=\frac{1}{2}\Big(\frac{H}{LA}+\frac{H}{LB}\Big)\geqslant s_0(LA\neq 0,LB\neq 0)\qquad(3)$$

若 $L_A=0$,$L_B=0$,定义 $\mathrm{sim}_{\mathrm{DNS}}=-1$,表示该域为僵尸服务器,将其域名加入到黑名单;若 $\mathrm{sim}_{\mathrm{DNS}}=0$,则表示域名合法,将域名加入白名单,并在域的 IP 列表中删除。假定有一个域名 DN 在时刻 t 被多个 IP 查询,可以通过监测在 t 之后的每一个时间间隔内,是否还被多个 IP 查询,来判断它是否是僵尸服务器。僵尸网络服务器的 $\mathrm{sim}_{\mathrm{DNS}}$ 一般接近于 1。根据中心的多次

监测,一般大于 0.8 比较能反映真实情况。

3　验证

3.1　Behavior-Domain 的监测实验

实验在部署于某市运营商机房 DNS 缓存服务器上进行,实验数据来自 DNS 缓存服务器的 DNS 流量镜像,采集程序对采集的数据按照请求及响应分开存放。

实验对象:修改了源码的采取 IRC、P2P 等协议的 botnet。修改以上常见的各类 bot 源码,移除 bot 的攻击破坏功能,并确保它们只能和实验中的服务器相连接。实验环境:Windows XP 操作系统下利用 Ethereal V1.2.4 作为抓包工具。监测系统根据监测模型在 Visual Studio 6.0 平台下使用 VC + +语言实现。

实验 1　选取网络上 4 个正常的 IRC、P2P 网络流量样本,测试 Behavior-Domain 模型对正常的网络流的判别检验情况。对于正常的 IRC、P2P 流量,得到的结果如表 1 所示。

表 1　Behavior-Domain 对正常流量的监测结果

类型	长度/M	持续时间/s	发包数	TCP 数据流	服务器	不成功数
Sample-IRC	5	180	23407	201	4	0
Sample2-IRC	23	2400	129632	927	4	0
Sample3-P2P	744	500	105530	8916	258	3
Sample4-P2P	1030	870	193413	4439	82	1
False Rate			(3 +1)/(4 +4 +258 +82) =1.15%			

结果表明, Behavior-Domain 模型对正常的 IRC、P2P 流量监测能取得较好的效果,误报率低至 1.15% 。

实验 2 在已经植入 bot 的环境下进行,对部署好的僵尸网络进行监测,实验结果如表 2 所示。

表 2　Behavior-Domain 对 botnet 的监测结果

类型	长度/M	持续时间/s	僵尸数	能否被监测	行为聚类流	域名聚类流	监测率/%
Unkown	463	1440	100	Yes	87	96	96
Sdbot	6	39	100	Yes	92	98	98
Spybot	57	154	100	Yes	89	100	100
Storm	2048	1440	500	Yes	478	499	99.8
Nugache	2048	1440	500	Yes	496	498	99.6

实验对植入的 1 种未知 bot 及 4 种常见 bot 的僵尸网络进行监测,通过对其网络流量的提取和分析,可监测到 botnet 的存在,监测率分别为 96% 、98% 、100% 、99.8% 、99.6% 。从实验结果可得, Behavior-Domain 监测模型对常见 bot 以及未知 bot 的僵尸网络具有较好的检测效果。但是,对未知 bot 的监测有效性要稍低于对已知 bot 的监测。

3.2　Behavior-Domain 与经典模型的比较

对比一些经典模型,针对基于 botnet 监测系统能否监测未知的 bot、监测活动能否独立于协议和结构、能否进行实时监测三个方面,对 Behavior-Domain 监测模型进行功能的定性评价,如表 3 所示。

表 3　Botnet 监测技术的比较

序号	基于 DNS 的监测策略	监测未知的 bot	独立于协议 & 结构	实时监测
1	Dagon D	True	Flase	Flase
2	Kristoff J	True	Flase	Flase
3	Schonewille A	True	Flase	Flase
4	Ramachandran N F A	True	Flase	True
5	This Article	True	True	True

表 3 所列出的几种监测模型都能监测未知的 bot。但是模型 14 仅仅只能针对使用某一种协议和结构的僵尸网络进行监测,一旦僵尸程序改变了自身的协议和结构,则监测方法失效。在实时监测方面,模型 13 均不具备实时监测功能。而 Behavior-Domain 模型能较好解决以上模型的功能欠缺问题。

4　结束语

为了实现在多协议和结构条件下进行僵尸网络实时监测,本文提出了一种利用 bot 行为和 bot 域名查询分析联动的监测方法。在实验中,首先通过对 botnet 的普遍行为进行监视,取得活动日志并聚类;其次通过对 bot 域名请求应答的监视,取得域名查询日志并聚类;最后将二次聚类的结果进行二次聚类分析。实验证明本文模型能监测到未知 botnet,能实时监测且不受 bot 的协议和结构限制。相比经典的监测方法,在监测的可扩展性和实时性上具有更好的效果。

参考文献:

[1] RACINE S. Analysis of Internet relay chat usage by DDoS zombies [D]. Zurich, Swiss: Swiss Federal Institute of Technology, 2004.

[2] CHEN Y. IRC-based botnet detection on high speed routers [C]// Proc of RO-DARPA-DHS Special Workshop on Botnets. 2006: 78-83.

[3] GOEBEL J, HOLZ T. Rishi: identify bot contaminated hosts by IRC nickname evaluation [C]// Proc of the 1st Workshop on Hot Topics in Understanding Botnets. Berkeley, CA: USENIX Association, 2007: 1-12.

[4] BINKLEY J, SINGH S. An algorithm for anomaly-based botnet detection [C]// Proc of the 2nd USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet. Berkeley, CA: USENIX Association, 2006: 43-48.

[5] ZHU Z, LU G, CHEN Y, *et al*. Botnet research survey [C]// Proc of the 32nd Annual IEEE International Conference on Computer Software and Applications. Washingtom DC: IEEE Computer Society, 2008: 967-972.

[6] RAJAB M, ZARFOSS J, MONROSE F, *et al*. A multifaceted approach to understanding the botnet phenomenon [C]// Proc of the 6th ACM-SIGCOMM Conference on Internet Measurement. New York: ACM Press, 2006: 41-52.

[7] DAGON D, GU G, LEE C P, *et al*. A taxonomy of botnet structures [C]// Proc of the 23rd Annual Computer Security Applications Conference. [S. l.]: Springer-Verlag, 2007: 325-339.

[8] DAGON D. Botnet detection and response, the network is the infection [J/OL]. http://www.caida.org/workshops/dns-oarc/200507/slides/oarc0507-Dagon.pdf.

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

[10] KRISTOFF J. Botnets [C]// Proc of the 32nd Meeting of the North American. 2004: 33-37.

[11] SALOMON R V, BRUSTOLONI J C. Identifying botnets using anomaly detection techniques applied to DNS traffic [C]// Proc of the 5th IEEE Consumer Communications and Networking Conference. [S. l.]: IEEE Press, 2008: 476-481.

[12] SCHONEWILLE A, Van HELMOND D J. The domain name service as an IDS [R]. Amsterdam: University of Amsterdam, 2006.

[13] RAMACHANDRAN N F A, DAGON D. Revealing botnet membership using DNSBL counter-intelligence [C]// Proc of the 2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet. 2006: 49-54.