P2P僵尸网络跨域体系结构的构建与评估

度宇鹏[1,2],张永铮[1,2],尹 涛[1,2]
(1.中国科学院信息工程研究所,北京 100093;2.中国科学院大学网络空间安全学院,北京 100049)

摘 要: 针对现有P2P僵尸网络抗追踪性较差的问题,提出了一种P2P僵尸网络跨域体系结构(CRA).CRA将僵尸主机间的通信严格限制在不同的域之间,并引入IP伪造技术隐藏通信的源IP.考虑到监控全球互联网的不可行性以及IP溯源的困难性,现实中防御者将很难对CRA展开追踪.模拟实验结果表明,较之当前主流的P2P僵尸网络体系结构,CRA具备更好的抗追踪性和鲁棒性.

关键词: 僵尸网络;体系结构;跨域;IP伪造;抗追踪
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2018)04-0791-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.04.004

Modeling and Evaluating a Cross-Realm Architecture for P2P Botnet

TUO Yu-peng[1,2],ZHANG Yong-zheng[1,2],YIN Tao[1,2]
(1. *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*;
2. *School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: To construct a tracking-resistant P2P botnet, a Cross-Realm Architecture (CRA) was proposed. CRA strictly restricts bots' interactions across different realms and hides the origins of bots' interactions by IP spoofing. Considering the infeasibility of monitoring the global Internet and the difficulty of IP traceback, it is very hard for defenders to track CRA in the real world. The simulation results show that compared to recent popular P2P botnet architectures, CRA has better anti-tracking performance and robustness.

Key words: botnet; architecture; cross-realm; IP spoofing; anti-tracking

1 引言

僵尸网络已成为互联网面临的最大安全威胁之一,它常被用来发起各种形式的网络攻击,如分布式拒绝服务攻击、窃取敏感信息、传播垃圾邮件等[1].早期的僵尸网络普遍采用集中式体系结构,这种体系结构存在单点失效的问题,一旦中心服务器被追踪到,则僵尸网络将被斩首[2].如今,P2P体系结构因其鲁棒性强的优势而被僵尸网络广泛采用.P2P体系结构允许攻击者从任意僵尸主机注入命令,从而避免了单点失效的问题,也增强了攻击者的隐蔽性.

近年来,随着图追踪方法[3~5]的提出,P2P体系结构抗追踪性较差的问题也随之暴露.问题的关键在于:P2P僵尸网络复杂的命令控制(C&C:Command and Control)机制不可避免地引起僵尸主机频繁地相互联系,而图追踪方法正是基于僵尸主机间的相互联系,提取用于识别P2P僵尸网络的通信特征,进而利用特定的算法从网络通信图中追踪P2P僵尸网络通信子图.Coskun B等人[3]认为网络内部属于同一P2P僵尸网络的僵尸主机,在网络外部有"朋友"(共同联系的僵尸主机)的概率远远高于正常主机,进而基于"共同联系"提出了"dye pumping"算法,根据已知僵尸主机追踪网络内部与其属于同一P2P僵尸网络的潜在僵尸主机.实验证明,该方法具有较高的准确率和召回率.François J等人[4]认为P2P体系结构中僵尸主机之间的通信模式具有高辨识度,并利用PageRank[6]算法对僵尸网络进

收稿日期:2016-09-19;修回日期:2017-04-18;责任编辑:李勇锋
基金项目:国家自然科学基金(No.61572496)

行追踪. 实验证明,在已知5%的僵尸主机前提下,该方法的准确率达到99%,误报率仅为0.1%. Nagaraja S等人[5]认为P2P僵尸网络的拓扑结构具有fast-mixing特性[7~10],并提出了BotGrep算法,迭代地将网络通信图划分为faster-mixing和slower-mixing子图,并最终缩小到fast-mixing子图,其中,包含已知僵尸主机的fast-mixing子图,被认为是P2P僵尸网络通信图. 实验证明,该方法能够以低于0.6%的误报率追踪到93-99%的僵尸主机.

为了提升现有P2P僵尸网络的抗追踪能力,本文从改变传统C&C通信模式入手,将C&C通信严格限制在不同域的僵尸主机之间,并且引入IP伪造技术隐藏C&C通信的源IP,使防御者很难从网络通信图中追踪到僵尸网络通信子图. 本文的主要贡献如下:

(1)提出了一种跨域体系结构模型(CRA),其中任意邻接节点颜色(域)不同. CRA融合IP伪造、数字签名及加密技术,实现了一种高安全的C&C通信机制,能够有效防回溯、防劫持、防窃听、防重放.

(2)提出了CRA的构建算法,其复杂度受节点分布影响,但最坏情况下仍能以$O(n^2)$的时间复杂度完成CRA的构建. 仿真实验表明,相比两种主流的P2P僵尸网络体系结构(TDL-4[5]、ZeroAccess[6]),该算法构建的CRA具有更好的抗追踪性和鲁棒性.

2 CRA模型

2.1 背景知识

众所周知,全球互联网可按不同维度划分为许多个域. 例如,按地域(国家/省份/城市…)划分、按自治域(AS)划分、按互联网服务提供商(ISP)划分等等. 每个域具有统一的管理机构和路由策略,且各个域之间相互独立. 欲对多个域进行监控,需要域间协作. 特别地,监控全球互联网在现实中具有不可行性. 图1以AS为域,给出了对互联网进行划分的示意图,其中,仅AS4、AS5和AS6为监控域,其余均为非监控域.

基于对僵尸网络分布情况的调研[11~14],我们发现僵尸网络在全球多个域中呈现出非均匀分布的特点. 而对防御者来说,仅监控域内僵尸主机的相互联系对其可见,因此限制域内僵尸主机相互联系有助于提升僵尸网络的抗追踪性. 在此基础上,若僵尸主机利用伪造的IP地址相互联系,则会进一步提升僵尸网络的抗追踪性.

2.2 模型描述

我们用染色的有向图$G(V,E,C)$描述CRA,其中,V表示节点集,每一个节点表示一台僵尸主机;E表示边集,边$<v_i,v_j>$表示源节点v_i用伪造的IP地址向目标节点v_j发起C&C通信;C表示颜色集,每种颜色代表一个不同的域. CRA不仅继承了传统P2P体系结构的属性,还融入了新的特性. 概括起来,我们提出CRA的两个基本特性:

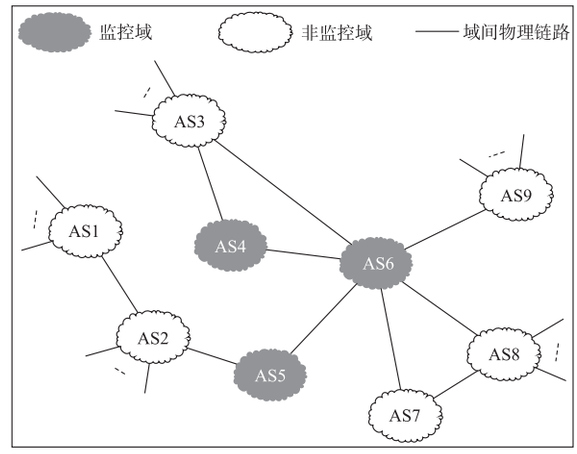


图1 互联网AS级划分示意图

1)跨域性:CRA中任意一条边的两个端点颜色不同. 这是CRA与传统P2P体系结构最大的区别,其目的是降低CRA内部联系被监控的风险,增强其抗追踪性.

2)强连通性:图G必须是强连通图,即图G中存在一条经过每个节点至少一次的回路. 这是CRA继承的P2P体系结构特性,即命令从图G中任意节点注入,均可覆盖到所有节点.

根据上述描述,图2(b)给出了一个CRA模型的示例,其中包含8个节点,3种颜色(黑色、白色、灰色). 从图2(b)中可以看出,存在一条延顺时针方向经过每个节点至少一次的回路,且每条边的两个端点颜色均不相同. 因此,该示例满足CRA的跨域性和强连通性.

2.3 命令控制机制

C&C机制是僵尸网络运作的核心机理. CRA采用PUSH式C&C机制,节点平时处于被动监听状态,当接收到C&C消息后,再向其下一跳节点转发,直至消息覆盖所有节点. 在消息传播的过程中,主要面临两方面的安全问题:一是僵尸网络劫持,即敌手可能冒充控制者向CRA中注入虚假命令,从而劫持僵尸网络;二是僵尸网络窃听,即敌手可能捕获某个节点,掌握其通信密钥,从而窃听CRA内部的C&C通信.

针对上述问题,我们设计了身份认证及个性化加密相结合的方案. 对CRA中的任意节点v,其属性可用五元组表示为:($v.ip$,$v.color$,$v.K^{'}$,K^{+},$v.peerlist$). 其中,$v.ip$表示对应僵尸主机的IP地址;$v.color$表示对应僵尸主机所属的域;$v.K^{'}$表示对应僵尸主机生成的对称密钥,用以加密C&C消息;K^{+}表示控制者的公钥,事先被硬编码在所有僵尸程序中,用以验证控制者身份;$v.peerlist$表示v的下一跳信息,用以路由C&C消息,记

为:$v.peerlist = \{(w.ip, w.K') \mid \forall <v,w> \in E\}$. 下面,分步讲解命令控制流程:

(1)消息注入:控制者任选一个节点,设为 v,然后伪造 IP 地址向其注入 UDP 消息:$E_{v.K}((seq + CMD) \| E_{K^-}(seq + CMD))$. 其中,$E_{v.K'}$ 表示用 $v.K'$ 加密;seq 为命令序号,逐次递增;CMD 为命令内容;E_{K^-} 表示控制者用其私钥 K^- 签名.

(2)消息认证:v 接收到消息后,首先用 $v.K'$ 解密得到 $(seq + CMD) \| E_{K^-}(seq + CMD)$. 然后用 K^+ 解密 $E_{K^-}(seq + CMD)$,若明文不为 $(seq + CMD)$,则控制者未通过身份认证,丢弃消息;否则进一步认证 seq,若为旧命令,则丢弃消息;否则执行命令并转步骤 3).

(3)消息转发:消息认证无误后,v 再向其下一跳节点集转发消息. $\forall (w.ip, w.K') \in v.peerlist$,$v$ 重新封装消息:$E_{w.K'}((seq + CMD) \| E_{K^-}(seq + CMD))$,然后用伪造的 IP 地址向 $w.ip$ 发送上述格式的 UDP 数据包.

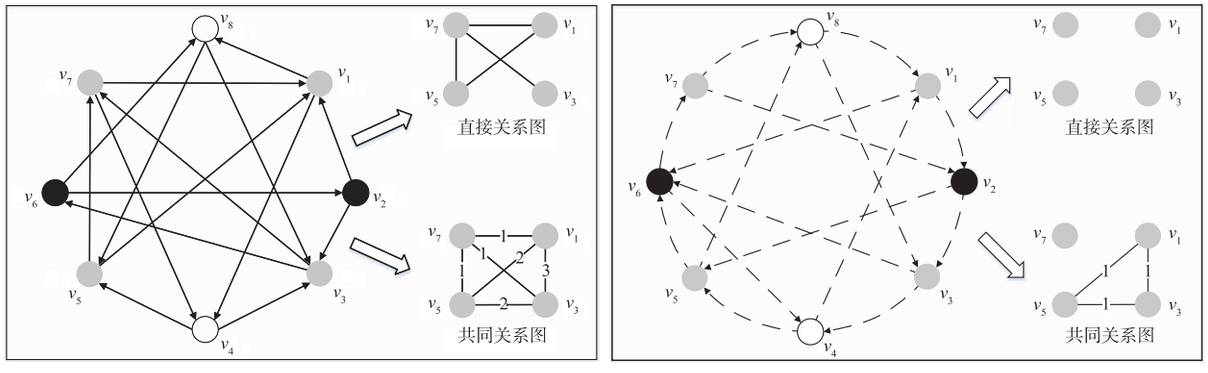
上述 C&C 通信方案可有效解决控制者身份认证问题,防止敌手劫持僵尸网络. 由于每个节点独立生成对称密钥 K',即便敌手捕获了某个节点,也至多掌握该节点及其下一跳节点的会话密钥,因此,能够有效防止敌手窃听 CRA 中其余节点间的 C&C 通信. 此外,设置命令序号 seq 不仅可以避免节点反复转发同一消息,还能够防止重放攻击.

2.4　与传统 P2P 体系结构的区别

CRA 与传统 P2P 体系结构有两大本质区别:1)CRA 中的 C&C 通信被严格限制在不同域之间,而传统 P2P 僵尸网络体系结构普遍没有限制;2)CRA 中的 C&C 通信源 IP 地址全是伪造的,而传统 P2P 僵尸网络普遍采用真实的 IP 地址. 为了突出 CRA 在抗追踪性上的优势,图 2 给出了 CRA 与传统 P2P 僵尸网络体系结构在同等条件(相同节点数、边数、域数)下的对比示意图.

假设灰色域受到防御者监控. 如图 2(a)所示的传统 P2P 体系结构中,节点采用真实的 IP 地址相互联系,防御者可推导出 v_1、v_3、v_5、v_7 之间的直接联系图. 更进一步,还可推导出灰色节点之间的共同联系图,边上的权重代表对应灰色节点在域外拥有的“朋友”数量. 相比之下,如图 2(b)所示的 CRA 模型具备跨域性,防御者无法导出灰色节点之间的直接联系图. 又由于每条边上的源节点 IP 地址都是伪造的,因此当且仅当域外某个节点同时指向多个灰色节点时(如边 $<v_8, v_1>$、$<v_8, v_3>$),防御者才有可能找到对应灰色节点之间的“朋友”,一定程度上增加了防御者导出共同关联图的难度. 但若节点每次伪造不同的 IP 地址向其目标节点转发 C&C 消息,则防御者几乎不可能导出共同联系图.

综上所述,相比传统 P2P 僵尸网络体系结构,CRA 在抗追踪性上有显著的优势.



(a)传统P2P体系结构模型　　(b)CRA模型

图2　抗追踪性对比

3　CRA 构建算法

假设图 G 包含 $v_0, v_1, \cdots, v_{N-1}$ 共 N 个节点,分布在 M 个域中($N >> M >> 1$),我们分两步构建 CRA:

(1)构建回路:首先从 v_0 出发,构建一条包含所有节点的回路,且回路中任意邻接节点的颜色均不同.

(2)随机加边:从 v_0 开始遍历回路,以当前节点为源节点,随机挑选 $K(K >> N)$ 个节点为目标节点. 若源节点和目标节点颜色不同,则添加一条边. 随机加边的过程,会增强 CRA 的鲁棒性,但同时也会加强节点间的联系,降低 CRA 的抗追踪性,这是一个性能间的平衡问题.

基于上述构建步骤,算法 1 给出了 CRA 构建算法的伪代码. 回路构建(02 ~ 15)的时间复杂度主要取决于 while 循环(07 ~ 12)的执行次数. 最好情况下,while 循环不执行,时间复杂度为 $O(n)$. 最坏情况下,while 循环执行 n 次,时间复杂度为 $O(n^2)$. 由于 K 为常数,且 $K << N$,因此,随机加边(16 ~ 23)的时间复杂度为 $O(n)$. 整体上看,算法 1 的时间复杂度取决于构建回路的过程,最好情况下,时间复杂度为 $O(n)$;最坏情况下,时

间复杂度为 $O(n^2)$.

算法 1 CRA 构建算法

```
输入:K;v0,v1,…,vN-1
输出:A   #CRA 的邻接矩阵
01  A ← Zeros(N,N)              #初始化为全 0 矩阵
02  for i ← 0 to (N-1) do       #构建回路
03    j ← (i + 1) % N
04    if vi.color≠vj.color then
05     A[i][j] ← 1
06    else
07      while true
08        k ← random(0,N-1)
09        if vk.color≠vi.color then
10          break
11        end if
12      end while
13      A[i][k] ← 1,A[k][j] ← 1
14    end if
15  end for
16  for i ← 0 to (K-1) do       #随机加边
17    for j ← 0 to (N-1) do
18      k ← random(0,N-1)
19      if vj.color≠vk.color then
20        A[j][k] ← 1
21      end if
22    end for
23  end for
```

4 实验与评估

4.1 数据集

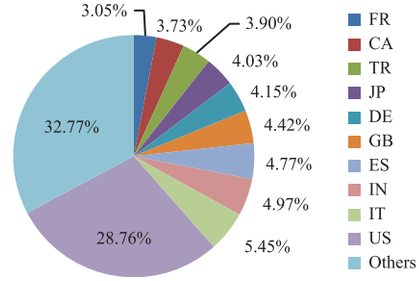
4.1.1 僵尸网络分布数据

以国家(用 ISO 3166-1[15]代码标识)为域,我们分别采集到 ZeroAccess[11]和 TDL-4[12]这两种近年来较为流行的 P2P 僵尸网络在全球多个域中的分布数据,如图 3 所示. 从图 3 可以看出,僵尸网络在全球多个域中呈现出非均匀分布的特点. 由于相关资料只公布了僵尸主机占有率排名靠前的若干个域,因此,后续讨论中我们统一将“Others”视为一个特殊的域.

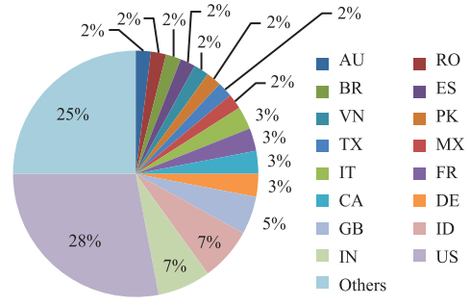
4.1.2 拓扑数据

ZeroAccess 采用分层的非结构化 P2P 体系结构,僵尸网络节点被分为超级节点和普通节点. C&C 消息在超级节点间以广播的形式传播,其体系结构和 Gnutella 网络[16]具有较高的相似性. 因此,我们采用 Gnutella 网络的拓扑数据仿真 ZeroAccess,数据来源于斯坦福大学公开的大规模网络数据集[17].

TDL-4 采用结构化 P2P 体系结构,其 C&C 通信基于 Kademlia[18]协议. 我们基于 PeerSim 平台[19]模拟了



(a) ZeroAccess分布数据



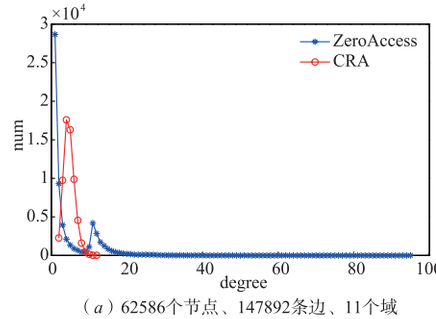
(b) TDL-4分布数据

图3 ZeroAccess和TDL-4的分布数据

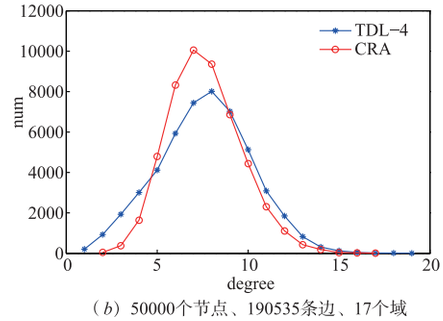
Kademlia 协议,并利用 TDL-4 的相关参数仿真其体系结构,最终以采样的方式获取其拓扑数据.

4.2 度分布

我们分别利用采集到的 ZeroAccess 和 TDL-4 的数据集,在同等条件下(相同节点数、边数和域数)构建了 CRA,并统计了它们的度分布情况,结果如图 4 所示.



(a) 62586个节点、147892条边、11个域



(b) 50000个节点、190535条边、17个域

图4 度分布情况

从图 4 可以看出,ZeroAccess 度分布在 1 ~ 95 之

间,其中度高于 12 的节点占 10.74%,度低于 3 的节点占 60.67%;而 CRA 度集中分布在 2 ~ 12 之间,且其中 92.73% 的节点度分布在 3 ~ 7 之间. TDL-4 度分布在 1 ~ 19 之间,其中 95.06% 的节点度分布在 3 ~ 12 之间;而 CRA 度分布在 2 ~ 17 之间,其中 95.58% 的节点度分布在 4 ~ 11 之间.

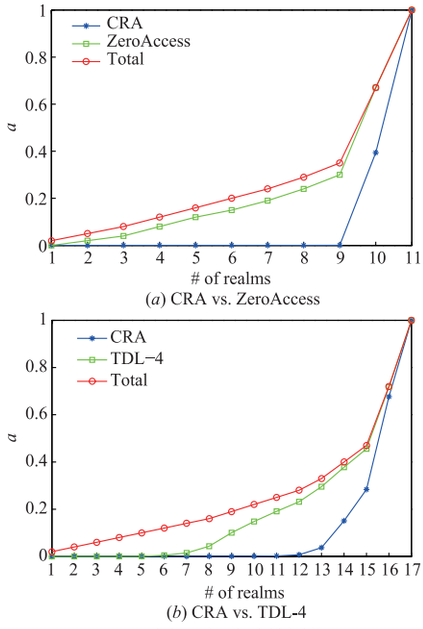
4.3　性能评估

4.3.1　抗追踪性

僵尸网络的抗追踪性用于评估僵尸网络抗追踪能力的强弱,与防御者的监控范围密切相关. 对图 3 中的每种僵尸网络,我们按照占有率从小到大的顺序,从 1 开始对域进行编号. 记 G_i 为图 G 投影在前 i 个域内的子图,它由所有位于前 i 个域内的节点及相关的边构成;记 $MCS(G_i)$ 为图 G_i 中的最大连通子图;记 M 为域的数量. 本文用于评估抗追踪性的表达式如下:

$$\alpha(i)=\frac{MCS(G_i)\text{中节点数量}}{G\text{中节点数量}}(1\leqslant i\leqslant M) \qquad (1)$$

其中,$\alpha(i)$ 表示当防御者拥有对前 i 个域的监控权时,僵尸网络的抗追踪性. α 越小,抗追踪性越强. 我们分别将 CRA 与其余两种僵尸网络在同等条件下进行了对比,抗追踪性的评估结果如图 5 所示.



(*a*) CRA vs. ZeroAccess

(*b*) CRA vs. TDL-4

图5　抗追踪性评估

图 5 中,Total 曲线表示僵尸主机在域上的累计占有率. 若 α 曲线越靠近 Total 曲线,则对应体系结构的抗追踪性越差. 实验结果表明,在同等条件下,CRA 的抗追踪性要好于其余两种 P2P 僵尸网络体系结构.

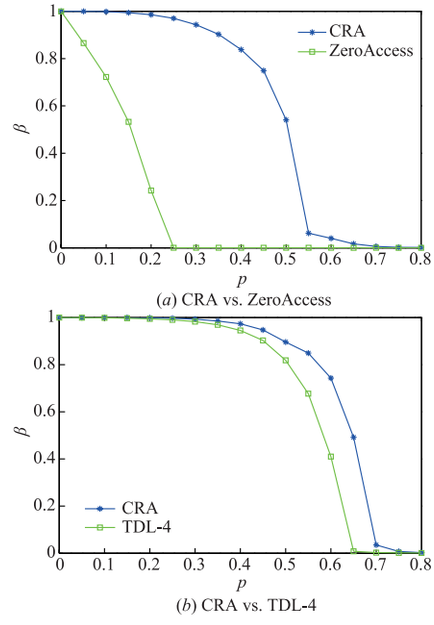
4.3.2　鲁棒性

僵尸网络的鲁棒性用于评估僵尸网络在面临节点不同程度失效的情况下,剩余部分的连通性. 影响僵尸网络连通性的因素主要有两个:(1)僵尸主机被防御者移除;(2)僵尸主机下线(例如:关机). 这两种因素虽然截然不同,但其对僵尸网络连通性的影响是相同的. 因此,在接下来的讨论中我们并不区分它们.

记 $G(p)$ 为移除图 G 中 p 部分节点及其相关的边后得到的子图,记 $MCS(G(p))$ 为图 $G(p)$ 中的最大连通子图. 本文用于评估鲁棒性的表达式如下:

$$\beta(p)=\frac{MCS(G(p))\text{中节点数量}}{G\text{中节点数量}}(0\leqslant p\leqslant 1) \qquad (2)$$

实际评估时,我们每次从图 G 中移除度最高的 p 部分节点(对网络连通性破坏最大),实验结果如图 6 所示.



(*a*) CRA vs. ZeroAccess

(*b*) CRA vs. TDL-4

图6　鲁棒性评估

实验结果表明,CRA 的鲁棒性比其余两种僵尸网络好,TDL-4 的鲁棒性强于 ZeroAccess. 我们认为,鲁棒性与节点的度分布密切相关. 在同等条件下,度分布越均匀,则僵尸网络的鲁棒性越好. 从图 4 的统计数据可以看出,在同等条件下,较之其余两种僵尸网络,CRA 的度分布更均匀,因此 CRA 的鲁棒性更好. 由于 ZeroAccess 中存在少部分度较高的超级节点,因此,在移除度最高的部分节点后,其鲁棒性直线下降.

5　结论

本文提出了一种僵尸网络跨域体系结构(CRA),其核心思想是将 C&C 通信严格限制在不同域之间,并引入 IP 伪造技术隐藏 C&C 通信的源 IP. 考虑到监控全球互联网的不可行性以及 IP 溯源的困难性, CRA 能显著提升现有 P2P 僵尸网络的抗追踪能力. 在模拟实验中,我们结合 ZeroAccess 和 TDL-4 的真实分布数据,基

于公开平台分别仿真了其体系结构,并在同等条件下,将其与 CRA 进行了对比. 实验结果表明,较之这两种僵尸网络的体系结构,CRA 具有更强的抗追踪性和鲁棒性.

参考文献

[1] Yu S,Guo S,Stojmenovic I. Can we beat legitimate cyber behavior mimicking attacks from botnets? [A]. INFOCOM 2012[C]. USA:IEEE,2012. 2851 – 2855.

[2] Nadji Y,Antonakakis M,Perdisci R,et al. Beheading hydras:performing effective botnet takedowns[A]. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security[C]. ACM,2013. 121 – 132.

[3] Coskun B,Dietrich S,Memon N. Friends of an enemy:identifying local members of peer-to-peer botnets using mutual contacts[A]. Proceedings of the 26th Annual Computer Security Applications Conference[C]. ACM,2010. 131 – 140.

[4] François J,Wang S,State R,et al. BotTrack:tracking botnets using NetFlow and PageRank[J]. NETWORKING,2011,2011:1 – 14.

[5] Nagaraja S,Mittal P,Hong C Y,et al. BotGrep:Finding P2P Bots with Structured Graph Analysis[A]. USENIX Security Symposium[C]. ACM,2010. 95 – 110.

[6] Brin S,Page L. The PageRank citation ranking:bringing order to the Web[R]. Stanford Infolab,2006.

[7] Gkantsidis C,Mihail M,Saberi A. Random walks in peer-to-peer networks[A]. INFOCOM 2004[C]. IEEE,2004. 1 – 12.

[8] Borisov N. Anonymous routing in structured peer-to-peer overlays[D]. University of California,Berkeley,2005.

[9] Aspnes J,Wieder U. The expansion and mixing time of skip graphs with applications[A]. Proceedings of the 17th Annual ACM Symposium on Parallelism in Algorithms and Architectures[C]. ACM,2005. 126 – 134.

[10] Zhong M,Shen K,Seiferas J. Non-uniform random membership management in peer-to-peer networks[A]. INFOCOM 2005[C]. IEEE,2005. 1151 – 1161.

[11] Golovanov S,Soumenkov I. TDL4 top bot[R]. Kaspersky Lab Analysis,2011.

[12] Neville A,Gibb R. Zeroaccess indepth[R]. Symantec Security Response,2013.

[13] Stone-Gross B. The lifecycle of peer-to-peer (gameover) zeus[R]. Dell Secure Works,2012.

[14] Kerkers M,Santanna J J,Sperotto A. Characterisation of the Kelihos. B Botnet[A]. IFIP International Conference on Autonomous Infrastructure,Management and Security[C]. Springer,2014. 79 – 91.

[15] International Organization for Standardization (ISO) 3166 – 1 [EB/OL]. https://en. wikipedia. org/wiki/ISO_3166 – 1,2017-4-19.

[16] Ripeanu M. Peer-to-peer architecture case study:Gnutella network[A]. Proceedings of First International Conference on Peer-to-Peer Computing[C]. IEEE, 2001. 99 – 100.

[17] Leskovec J,Krevl A. SNAP Datasets:Stanford large network dataset collection (2014)[OL]. http://snap. stanford. edu/data.

[18] Maymounkov P,Mazieres D. Kademlia:A peer-to-peer information system based on the xor metric[A]. International Workshop on Peer-to-Peer Systems[C]. Springer, 2002. 53 – 65.

[19] Montresor A,Jelasity M. PeerSim:A scalable P2P simulator[A]. Ninth International Conference on Peer-to-Peer Computing 2009[C]. IEEE,2009. 99 – 100.

作者简介

庹宇鹏 男,1984 年出生,河北廊坊人,中国科学院信息工程研究所助理研究员,主要研究方向为网络异常检测、移动互联网大数据挖掘.

E-mail:tuoyupeng@ iie. ac. cn

张永铮(通信作者) 男,1978 年出生,黑龙江哈尔滨人,博士,中国科学院信息工程研究所研究员、博士生导师,主要研究方向为网络安全态势感知.

E-mail:zhangyongzheng@ iie. ac. cn