



基于改进神经网络算法的木马控制域名检测方法

刘爱江¹, 黄长慧², 胡光俊²

(1.公安部科技信息化局 北京 100741; 2.公安部第一研究所 北京 100048)

摘要:首先对木马利用域名进行回连控制的特点进行了分析,对采用 DNS 进行网络木马检测的方法进行了概述,接着基于对木马域名的静态、动态特征的分析,提取了域名使用时间、访问域名周期性、IP 地址变化速度、IP 地址所属国变更、IP 地址为私有地址、同域名多 IP 地址分属不同国家、TTL 值、域名搜索量 8 个指标作为 BP 神经网络算法的输入,并提出了一种改进 BP 神经网络算法来解决大量 DNS 域名训练效率、平均误差值大的问题;最后用改进的神经网络算法对样本进行了实验评估测试,结果显示改进算法和传统算法的检出率相当,但检测效率大为提高。

关键词:木马病毒;域名;神经网络

doi: 10.3969/j.issn.1000-0801.2014.07.007

Detection Method of Trojan's Control Domain Based on Improved Neural Network Algorithm

Liu Aijiang¹, Huang Changhui², Hu Guangjun²

(1.The Bureau of Science and Technology Information of Ministry of Public Security, Beijing 100741, China;

2. The First Research Institute of Ministry of Public Security, Beijing 100048, China)

Abstract: Firstly, the character that the Trojans use domain name to control was analyzed and the method that DNS adopted to detect Trojans was introduced. Secondly, based on the analysis of static and dynamic characters for Trojan domain name, eight indicators were obtained as the input of BP neural network algorithm, including operation time of domain name, the period to visit the domain name, the variation speed of IP address, the country change of IP address, IP address of private address, the same domain name with multiple IP address for different countries, TTL value and search times of domain name. An improved BP neural network algorithm was proposed to solve training efficiency for a great number of domain names, and large average error. Finally, the experimental evaluation of samples was tested by improved neural network algorithm. Compared with traditional neural network algorithm, the detection efficiency is better.

Key words: Trojan, domain name, neural network

1 引言

DNS(domain name system,域名解析系统)协议是互联网的核心协议之一^[1],提供网络标识到 IP 地址的翻译服务,帮助网络用户顺利使用 Web 网站、邮件服务等在线服

务,DNS 协议也被木马服务端用来寻找解析控制服务器地址。木马攻击者在设计木马时,必须考虑木马攻击成功后如何能稳定快速地回连接收控制,或准确地回传获取的数据,如果采用固定 IP 地址,一旦该 IP 地址丢失将失去对木马的控制。域名一般相对固定,每次 IP 地址变化后,只



要重新绑定域名的 IP 地址,木马就能按照 DNS 协议解析域名,从而得到新 IP 地址实现成功回连。

恶意域名检测分为主动 DNS 分析和被动 DNS 分析两种方式。主动 DNS 分析一般用于对特定域名进行分析,通过主动查询 Whois 数据库、使用 Nslookup 工具查询域名参数获取信息来做出判断,由于需要在线查询数据库,所以速度较慢。被动 DNS 分析一般用于大规模 DNS 筛查,通过被动监听 DNS 请求,抽取其中特征,然后采用提前训练好的分类器对被检域名进行分析判断。Seifert 等人^[2]基于恶意域名的生存期较短、知名度较低、用户级 DNS 服务器没有相应的 DNS 解析信息、用户发出的 DNS 请求大部分会被重定向到根 DNS 服务器为前提,提出利用 DNS 递归查询率来发现恶意域名的方法。Choi 等人^[3]以分布式僵尸程序(Bot 程序)同时发来 DNS 查询形成的一个群组活动为前提,提出一种监测 DNS 请求异常的僵尸网络(BotNet)检测机制,但该方法在监测大规模网络活动时需要消耗极多时间。Foo 等人^[4]注意到 BotNet 使用的 DNS 指向的 IP 地址包含了相当比例的动态 IP 地址,如果不处理动态 IP 地址情况,将为 BotNet 度量带来很大的误差,于是提出动态 IP 地址识别问题,并通过 PTR(pointer)查询识别动态 IP 地址,可惜我国的宽带 IP 地址基本上都不支持 PTR 解析,限制了该方法的实际使用。Ramachandran 等人^[5]通过建模的方法将由僵尸控制者组织的 DNS 黑名单(DNSBL)列表查询与合法的 DNSBL 流区分开来以确定可能的 BotNet,该方法可以用来检测实时的侦查活动,但不能检测分布式的查询。Dagon 等人^[6]采用修改 DNS 配置,使 Bot 程序连接到蜜罐主机,而获得监测时间内的不同僵尸主机的 IP 地址数,从而测量 Botnet 的规模,但是由于动态 IP 地址及 NAT IP 地址和主机数无法对应,实际的僵尸程序数与该方法得到的数量有很大的差异。

2 木马回连 DNS 特征提取技术

首先对木马回连域名的特殊性进行分析。由于木马程序的特殊性,其回连使用的域名与正常网络应用使用的域名的行为特点有以下不同。

- 域名在 Whois 数据库中注册的申请时间不会很长。由于各大杀毒软件厂商都在针对木马回连域名构造查杀库,随着使用时间的增长,域名势必会暴露,之后攻击者必须申请新域名为木马连接所用,所以木马回连域名注册时间不会很久远。

- 木马为保证能快速、稳定回连,一般会采用循环连接的方式,如 5 min/回连一次,使得控制者可以及时看到在线的计算机。
- 由于经常使用 ADSL 等方式控制,木马回连域名对应的 IP 地址一般会经常变化,表现形式就是对同一个域名请求返回的 IP 地址经常是变化的。
- 木马在不使用时,常常会将域名对应的 IP 地址指向非受控 IP 地址,这个 IP 地址的选取一般是随机的,此时会看到域名指向的 IP 地址对应的国家会发生很大的变化。
- 木马在不使用时,有时会将域名指向私有 IP 地址,如 127.0.0.1、192.168.0.x 等,而正常的域名是不会解析成私有 IP 地址的。
- 木马使用多个 IP 地址指向一个域名做负载均衡时,多个 IP 地址一般位于不同的国家或地区,而这种情况对于正常的网站是极其罕见的。
- 由于 IP 地址经常变化,木马回连域名对应的 TTL (time to live)值一般会很短,否则会出现木马上线不稳定的现象。

通常的域名会采用有意义且易记忆的字符组合,而木马使用域名的目的是方便回连控制,并没有需要公众记忆的问题,同时由于短字符的域名被注册比例已经较大,所以木马回连使用的域名一般较复杂。

根据上述木马域名的请求特点,分析木马的 DNS 网络行为,选取 8 个指标,分别是域名使用时间、访问域名周期性、IP 地址变化速度、IP 所属国变更、IP 为私有地址、同域名多 IP 地址分属不同国家、TTL 值、域名搜索量。

(1)域名使用时间指标 $NsUseYear$ 的建立

域名使用时间是当年 $NowYear$ 与域名注册年 $NsCrYear$ 的差,计算方法为:

$$NsUseYear = \begin{cases} 5, & NowYear - NsCrYear \geq 5 \\ NowYear - NsCrYear \end{cases}$$

(2)访问域名周期性指标 $ViNsCycle$ 的建立

在给定的时间段内,相同源 IP 地址间隔同样时间连续 3 次以上访问同一域名,间隔时间为 $ViNsCycle$ 。设定给定时间段为 24 h,考虑到网络时延,间隔时间为 $ViNsCycle \pm 3$ s,设第 n 次域名访问时间为 $NsVisit_n$,间隔时间为 T_n ,则周期性算法如下:

$$ViNsCycle(NsVisit) \\ \{$$

$$T_1 = NsVisit_2 - NsVisit_1;$$

$$T_2 = NsVisit_3 - NsVisit_2;$$

$$T_3 = NsVisit_4 - NsVisit_3;$$

$$\text{If}((T_1 \pm 3) \leq T_2 \in \leq (T_1 \pm 3))$$

$$\text{If}((T_1 \pm 3) \leq T_3 \in \leq (T_1 \pm 3))$$

$$ViNsCycle = T_1$$

Then

$$ViNsCycle = 0$$

}

(3) IP 地址变化速度指标 $IpChSpeed$ 的建立

在给定的时间段内,同一域名对应的 IP 地址频繁变化, $IpChSpeed$ 为变化的次数与时间段的比。设给定时间段为 24 h,IP 地址变化次数为 $TimeChgIp$,则:

$$IpChSpeed = TimeChgIp/24$$

(4) IP 地址所属国变更指标 $IpCouCh$ 的建立

在一个时间段内,同一域名的 IP 地址进行了 1 次以上的变化,且前后 IP 地址位于不同的国家范围内,则 $IpCouCh$ 为 1,否则为 0。设定时间段长度为 24 h。

(5) IP 为私有地址指标 $IpIsPriv$ 的建立

在一个时间段内,同一域名的 IP 地址如果出现私有 IP 地址,则 $IpIsPriv$ 为 1,否则为 0。设定时间段长度为 24 h。

(6) 同域名多 IP 地址分属不同国家指标 $NsMulpCou$ 的建立

解析同一个域名得到多个 IP 地址,如果这几个 IP 地址分散在不同的国家则 $NsMulpCou$ 为 1,否则为 0。

(7) TTL 值指标的建立

取 SOA 查询类型得到的 default TTL 值 $DeTTL$ 计算 TTL:

$$TTL = \begin{cases} 600, & DeTTL \geq 600 \\ DeTTL \end{cases}$$

(8) 域名搜索量指标 $NsSearchNum$ 的建立

将域名作为关键词在 Google 中搜索,依据获得的结果数 $SearchNum$ 计算 $NsSearchNum$:

$$NsSearchNum = \begin{cases} 1\ 000, & SearchNum \geq 1\ 000 \\ SearchNum \end{cases}$$

3 基于改进神经网络算法的分类器设计

为解决大量 DNS 域名训练效率、平均误差值大的问题,本文提出一种改进的 BP(back propagation)神经网络算法。该算法对于不同的输入只激发部分神经元产生输出,被激发的神经元之间形成激发路径,在误差反向传播过程

中只调整激发路径上的权值。此算法可以降低平均误差并很好地改善算法的学习效率,应用到恶意域名的识别中,具有更高的恶意域名识别速度和识别率。设网络的输入层有 n 个神经元,两个隐含层,分别具有 k_1 和 k_2 个神经元,输出层有 m 个神经元,使用 sigmoid 函数作为神经元的激活函数,网络学习算法如下。

(1) 首先计算网络的实际输出。对于每个输入 $X=x_1, x_2, \dots, x_n$, 计算 BP 网络的实际输出 $Y=y_1, y_2, \dots, y_m$ 。

(2) 然后计算误差。对于第 p 个样本,假设样本的输出

为 $T=(t_{p1}, t_{p2}, \dots, t_{pm})$ 。误差函数是 $E_p = \frac{1}{2} \sum_{i=1}^m (t_{pi} - y_{pi})^2$ 。所有样本

的总误差为 $E = \sum_p E_p$ 。

(3) 接着对权值进行调整。利用梯度下降法来计算误差函数的极小值,权值 w_{ij} 的更新量 Δw_{ij} 可表示为:

$$\Delta w_{ij} \propto -\eta \frac{\partial E}{\partial w_{ij}}$$

其中, η 代表学习速率。

参考文献[7]中描述了一种学习网络的结构和算法,这种算法具有良好的功能分布特性。由于文中所提的学习网络与 BP 神经网络在结构、功能、训练算法上相似,所以本文借鉴其功能分布的基本思想,并在 BP 神经网络中加以实现,通过实验证明了这种方法是可行的,对恶意域名检测系统的效率有明显提升。功能分布思想的实践的核心是:在不同的输入下激发神经网络不同的部分,而被激发的神经元形成了一条激发路径,在此激发路径上进行误差反向传播。算法描述如下。

(1) 所有输入层的神经元被无条件激发。

(2) 各隐含层的神经元之间进行相互竞争,规定具有最大绝对输出值的神经元被激发,设每次前向过程的一次竞争中 n_l 个神经元被激发,这 n_l 个神经元的绝对输出值最大,其中 l 代表第 l 次竞争。若隐含层的数量为 L ,则最多有 L 次竞争。

(3) 所有输出层的神经元无条件被激发。

结束以上 3 个步骤,被激发的神经元的总数 $N(t)$ 为:

$$N(t) = \sum_{l=1}^L n_l + N_{in} + N_{out}$$

其中, N_{in} 为输入层神经元的总数量, N_{out} 为输出层神经元的总数量, $N(t)$ 个被激发的神经元形成激发路径。算法的核心思想是如果隐含层神经元被激发后的输出值很小,则



表 1 网络训练结果比较

训练时间		最小平均误差		检测率	
改进算法	传统算法	改进算法	传统算法	改进算法	传统算法
2 min 46 s	4 min 15 s	0.024 142	0.035 741	97.8%	96.4%

将其忽略。此算法与传统的 BP 神经网络算法相比,后者针对每个训练样本需要对网络上所有权值进行调整,而前者在确定训练样本的前提下,只对激发路径覆盖的权值进行调整,具有更高的训练效率。

4 实验与评估

试验数据包含正常域名和木马域名两部分。正常域名从 www.alexa.com^[8]获取,包括全世界访问量前 10 万个网站域名,前 6 万个用于训练,后 4 万个用于测试;木马域名从 www.malwaredomains.com^[9]获取,取 1.5 万个,前 1 万个用于训练,后 0.5 万个用于测试。

对于 115 万个域名,获取 *NsUseYear*、*ViNsCycle*、*IpChSpeed*、*IpCouCh*、*IpIsPriv*、*NsMulpCou*、*TTL*、*NsSearchNum* 8 个属性特征值作为网络的输入,然后使用传统算法和改进算法进行仿真。

域名检测 BP 网络的结构中,输入层的神经元数量为 8 个,隐含层为 2 层,均包含 10 个神经元,输出神经元数量为 1 个,改进算法的和值均设置为 4,代表每次竞争有 4 个神经元被激发。学习速率初始化为 0.15,动力因子为 0.075, $f(x)=1/(1+e^{-x})$ 。网络的初始权值和阈值定为 (-1.0, 1.0) 的随机数。

表 1 为训练时间和稳定时的最小平均误差。

从实验结果可以看出,改进的 BP 神经网络算法效率更高、最小平均误差更小且木马域名检出率更高。

参考文献

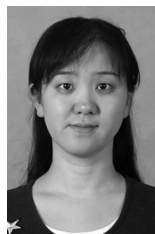
- 1 Mockapetris P. Domain Names-Concepts and Facilities. RFC1034, 1987
- 2 Seifert C, Welch I, Komisarczuk P, *et al.* Identification of malicious web pages through analysis of underlying DNS and web server relationships. Proceedings of the 33rd IEEE Conference on Local Computer Networks, Montreal, Canada, 2008: 935~941
- 3 Choi H, Lee H, Lee H, *et al.* Botnet detection by monitoring group activities in DNS traffic. Proceedings of the 7th IEEE International Conference on Computer and Information Technology (CIT'07), Washington, DC, USA, October 2007:715~720

- 4 Foo S, Hui S C, Yip S W, *et al.* Approaches for resolving dynamic IP addressing. Internet Research, 1997,7(3): 208~216
- 5 Ramachandran A, Feamster N, Dagon D. Revealing botnet membership using DNSBL counter-intelligence. Proceedings of the 2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet(SRUTI'06), San Jose, CA, USA, 2006:49~54
- 6 Dagon D, Zou C, Lee W. Modeling botnet propagation using time zones. Proceedings of NDSS, San Diego, California, USA, 2006
- 7 Hirasawa K, Oka S, Sakai S, *et al.* Learning Petri network with route control. Proceedings of IEEE International Conference on Systems, Man, Cybernetics, Vancouver, BC, Canada, 1995: 2706~2711
- 8 Alexa. <http://www.alexa.com/topsites>, 2012
- 9 mirror2.malwaredomains.com. <http://mirror2.malwaredomains.com/files/>, 2012

[作者简介]



刘爱江,男,公安部科技信息化局副局长,主要研究方向为信息安全。



黄长慧,女,公安部第一研究所工程师,主要研究方向为网络安全。



胡光俊,男,公安部第一研究所副研究员,主要研究方向为网络安全。

(收稿日期:2014-06-22)