武汉邮电科学研究院硕士学位论文

开题报告

专 业： 通信与信息系统

研究方向： 网络安全

论文题目：基于Fast-flux的DNS异常行为分析

研 究 生： 李骜骋 学号： 20150075

导 师： 王峥

报告日期： 2016年11月24日

|  |
| --- |
| 1. 课题的来源、目的及意义 |
| 域名系统（Domain Name System），简称DNS，是为用户提供域名和IP地址之间的映射提供服务。在目前互联网遍布广泛的情况下，DNS是不可或缺的一部分。在互联网中，很多应用都需要DNS的支持，DNS的安全性也很大程度上决定了互联网的安全性。从另一个角度来说，DNS的报文中也会包含用户的信息。因此，过滤DNS攻击报文，保证DNS运转的安全性，对于整个互联网系统的安全来说也是至关重要的。  近年来，DNS攻击事件层出不穷，造成的影响巨大，损失惨重。针对个人的攻击有 DNS劫持、DNS污染、钓鱼网站、植入后门等，个人的账户、密码等隐私信息被窃取以后，将遭受不必要的损失。针对组织而言，拒绝服务攻击、域名劫持、缓存污染等DNS攻击已经造成很多在社会范围内影响较大的事件。如09年发生的“5.19断网事件”，全国的互联网几乎都处于瘫痪状态。再如14年全国范围的大面积DNS服务器故障，若干家大型互联网公司，如百度、新浪这样的知名互联网公司，在几小时内无法提供服务。还有2016年发生的由美国东部起始的DNS攻击，大半美国都不能使用互联网。  DNS存在如此大范围的攻击主要是由于DNS本身存在漏洞。一方面，DNS是一个开放的系统，所有用户可以没有限制地使用该系统进行域名查询和应用，在用户使用过程中，该系统缺少必要的认证和加密机制，DNS客户端发送请求报文后，无法确认接收到的信息的真实性和可靠性，且DNS客户端仅认为接收到的第一条回复报文就是需要的内容，而很多DNS攻击正是利用这个特性欺骗并控制对应的主机。另一方面，DNS采用UDP协议，UDP类型报文的特点是尽最大能力交付，在DNS请求和应答过程中，请求报文和应答报文容易丢失或者受到欺骗。  现有的DNS攻击主要存在于僵尸网络中，僵尸网络（Botnet）是采用一种或者多种手段传播，将大量主机感染bot程序病毒，从而在控制者和被感染主机之间形成一个可一对多控制的网络。针对DNS攻击，主要有fast-flux和domain-flux两种技术，fast-flux技术是攻击者将域名快速变换，传播的DNS攻击包的最大生存时间非常短；Domain-flux技术主要是攻击者欺骗主机，替换正确报文中的IP地址的回复。由于两种技术的特征相差较大，很难用相同的方式进行检测，因此本文拟对特征较为明显的fast-flux攻击进行研究，并且将分析和检测主要集中在域名字符和相关报文特征上，帮助主机避开fast-flux僵尸网络的攻击。  本课题的目的：本文意在通过机器学习的相关算法技术，达到识别出fast-flux的攻击，削弱其攻击包的攻击性，同时维持正常的DNS的运行的目的。  本课题的意义：通过对DNS攻击识别，解决大量存在僵尸网络中的DNS攻击的问题，避免因DNS攻击而导致大面积网络不可用的局面；另一方面，保护用户的权益，使用户免遭损失，净化互联网环境，加强互联网安全。 |
| 1. 本课题的国内外研究现状及发展趋势分析   （在文献调研的基础上完成此部分内容，并列出至少10篇相关文献。） |
| DNS异常行为基本是僵尸网络所发起的攻击，利用fast-flux技术通过DNS欺骗、恶意域名等方式对主机或者本地服务器进行攻击[1]，导致DNS无法正常服务，甚至造成一定的损失。  就目前来看，为了逃避检测，僵尸网络中越来越多的出现新技术、新种类。其中fast-flux对DNS的攻击技术是被攻击者应用较为广泛的技术。Fast-flux是僵尸网络使用的一种快速变换IP地址的DNS攻击技术，早在2005年，D.Dagon等人就提出通过检测域名来定位僵尸网络命令和控制（C&C）信道服务器的方法[2]。在2007年起，fast-flux攻击收到关注并被广泛研究。康乐、李东等人基于SVM技术研究了fast-flux的僵尸网络检测技术[3],LASOTA等人[4]发现并分析了一种以DNS隧道为C&C的僵尸网络，从而引发了对这一类新型威胁的重视。另外，周昌令等提出了一种将DNS查询行为映射到向量空间的方法[5],钟霖甘研究在Linux环境下的DNS攻击检测。利用支持向量机的方法，设计了入侵检测系统，过滤有攻击性质的DNS报文[6]。上述提及的方式中算法的改进不多，如果针对应用的算法加以优化结果会更好。  另外，还有一部分通过挖掘恶意域名的特征，以实现更为通用的检测算法，例如SPRING J M等人[7]分析了恶意域名字符串构成的相似性，HAO S等人研究了恶意域名的早期初始DNS行为[8]。ANTONAKAKIS等人[9]则分析域名请求序列，从已知恶意软件域名跟踪与之相关的未知恶意域名。BILGE L[10]的Notos系统基于网络地址、DNS区和恶意线索三类特征，实现了一个动态的域名声望系统。ANTONAKAKIS M实现的EXPOSURE系统[11]则对请求时间特征、回答特征、TTL特征和域名特征进行机器学习，识别包括恶意软件、钓鱼网站在内的各类恶意域名。与Notos和EXPOSURE不同，CONRAD D的Kopis[12]部署在上层的授权域名服务器，基于查询者分布、查询者属性和解析IP声望挖掘恶意域名。以上基于DNS的恶意域名挖掘算法的设计目标与本文较为相似，但所涉及的特征比较少，如果在多维空间计算正确性会更高。  总体来说，DNS异常检测的相关研究工作还存在检测不及时、监控不全面等问题，这些问题导致网络攻击依然在时常发生，DNS的安全漏洞广泛地被黑客利用[13]，并在全球范围内造成了很大的危害和安全隐患，DNS的异常行为的研究还是很有必要继续稳步的开展下去。保护用户的权益，让用户免遭损失，净化互联网环境，加强互联网安全。  本文准备对基于fast-flux技术的DNS异常行为进行分析，从几十个特征维度进行降维和特征融合，提取DNS报文的特征，然后利用机器学习的方式，对特征进行二分聚类，找到并滤除有fast-flux异常行为的DNS报文，使带有异常行为的DNS报文无法对用户进行攻击。  参考文献：   1. 侯曼 Passive DNS系统的实现与应用研究[D] 北京邮电大学 2014 2. David Dagon. Botnet Detection and Response: the Network is the Infection[R]. In Proceedings of DNS Operations Analysis and Research Center. 2005:1-45 3. 康乐 基于SVM的Fast-flux僵尸网络检测技术研究[J] 智能计算机与应用2011 4. LASOTA K,KOZAKIEWICZ A. Analysis of the Similarities in Malicious DNS Domain Names[C].In The 1st FTRA International Workshop on Convergence Security in Pervasive Environments, Loutraki, Greece, June 28 30,2011:1 6 5. 周昌令 基于深度学习的域名查询行为向量空间嵌入[J] 通信学报 2016 6. 钟霖甘 基于SVM方法的DNS服务攻击防范模型[D] 复旦大学 2009 7. SPRING J M,METCALF L B,STONER E. Correlating Domain Registrations and DNS First Activity in General and for Malware[C].In Securing and Trusting Internet Names, NPL, Teddington, UK, April 4 5,2011. 8. HAO S,FEAMSTER N,PANDRANGI R. Monitoring the Initial DNS Behavior of Malicious Domains[C].In Internet Measurement Conference, Berlin, Germany, November 24,2011:269 278 9. ANTONAKAKIS M,PERDISCI R,DAGON D, el at. Building a Dynamic Reputation System for DNS [C].In 19th USENIX Security Symposium, Washington, DC, USA, Aug 11 13, 2010:273 290 10. BILGE L,KIRDA E,KRUEGEL C ,et al. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis[C].In 18th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, Feb 6 9,2011. 11. ANTONAKAKIS M,PERDISCI R,LEE W, el at. Detecting Malware Domains at the Upper DNS Hierarchy[C].In 20th USENIX Security Symposium, San Francisco, CA, USA, Aug 8 12,2011:27 27. 12. CONRAD D.A Quick Introduction to the Domain Name System[C].In ITU ENUM Workshop,Genva,Switzerland,Jan.17,2001. 13. 王天佐 僵尸网络中的关键问题[J] 计算机学报 2012 |
| 三、课题中待解决的关键问题 |
| 本文主要针对基于fast-flux技术的DNS攻击进行研究，先截获大量DNS报文，然后用Python的pcap包将DNS报文的内容解析出来，格式化存储在数据库中，根据DNS报文内容中对应的特征属性进行特征提取，识别出哪些DNS报文属于fast-flux异常甚至攻击行为，哪些DNS报文是主机正常请求的报文，最终在客户端过滤掉有fast-flux攻击嫌疑的DNS报文，并不影响主机的正常DNS请求响应。其中，待解决的关键问题有：  1、Fast-flux僵尸网络检测困难  Fast-flux（又称为IP-flux）僵尸网络是由一些被控制的计算机组成的系统，其公共DNS记录在持续变化且变化时间间隔非常短，这种DNS记录变化的机制使得犯罪行为更难追踪和阻断。  2、DNS报文的特征提取的维度灾难。  如果完全将DNS报文中的字段作为特征进行算法处理，将导致维度灾难，因此需要将DNS报文解析后的字段进行降维计算，提取最有用的特征，或者信息熵最大的几个特征，有些字段需要进行特征融合，提高字段可用性。  3、如何选择适合DNS特征的算法。  本文将利用机器学习的方法对报文进行识别分类，拟选取的算法有神经网络算法和SVM算法。由于未进行实际操作无法确定算法，需要针对本文的内容选择较为适合的算法，并在设计分类器的过程中找到算法的缺陷并进行改进。 |
| 四、课题的研究内容 |
| 本文主要针对DNS报文的异常行为分析，将报文的内容用机器学习的方法进行分析，找到在僵尸网络中具有fast-flux攻击的DNS报文与正常报文不同的异常行为，并归纳其特征，最后做出能够在客户端防范fast-flux攻击的识别系统。主要工作如下：  1、研究fast-flux攻击的相关技术共性。  僵尸网络是本文研究的大主题，僵尸网络的攻击特征，以及基于僵尸网络的fast-flux技术的学习是本文的基础。首先需要找出fast-flux攻击技术的特点，fast-flux僵尸网络是由一些被控制的计算机系统组成，这些计算机系统的公共DNS记录在持续变化，并且变化的时间非常短，需要针对这些特点以及相关的更多特点设计特征选择的方法。  2、特征提取。  解析后的DNS报文为特征的原始形式，将这些字段进行降维选取并处理得到需要使用的特征维度。特征的选取具体有三种形式：一种是直接将字段作为特征；另一种是将非数字形式的字段进行量化并归一化进行处理；第三种是结合其他字段进行特征融合形成新的特征维度。本文拟提取六个特征，即用六个维度表示DNS报文，在六维空间中对报文进行分类，区分带有fast-flux的攻击包和其他非攻击包。  3、PCA降维算法应用。  PCA（Principle Component Analysis）中文名是主成分分析，是目前应用最广泛的一种特征提取的方法之一，本文将使用PCA降维算法进行对报文的预处理，以达到减小分析维度并维持报文原始特征的目的。  4、选择的算法优化和改进。  通过学习和比较机器学习的算法，本文初步准备选用神经网络算法和支持向量机算法中的一个，两个都是分类算法，且两种算法均有较强的学习能力，可以通过利用这两种算法中的一个将带有fast-flux攻击的DNS报文与非攻击性的DNS报文区分开。本文先将两种算法都进行尝试计算，然后比较两种算法的结果，选出较为适合的算法，并根据计算过程中暴露的缺陷有针对性的对算法进行优化和改进，最终得到最适合本文样本的算法模型，并设计出基于本文的算法模型的分类器，最后给出分类器的结果并验证结果的有效性。 |
| 五、拟采取的研究方法、实验方案、技术路线 |
| 本文首先根据僵尸网络以及DNS检测的相关研究所采取的方法，利用PCA算法对提取的报文特征进行降维，将DNS报文的字段用主成分分析（PCA）算法进行降维，主成分的贡献率可用公式（1）表示  式（1）  主成分中方差较小或者较小的主成分被认为包含的是噪声，在分析时不使这些变量引入模型，这样使分析的主成分减少，以达到降维的目的。总的来说PCA是一种统计学方法，其基本思想是提取出空间原始数据中的主要特征（主元），减少数据冗余，优点是使得数据在一个低维的特征空间被处理，保持原始数据的绝大部分信息，解决数据空间维数过高的问题，应用于本文即是用于降维。  下一步，利用神经网络和支持向量机两种方法中选择一种较好的算法，并改进。  支持向量机的算法过程如下：  超平面公式 =  拉格朗日算子 L(,,α)=-  最优决策面 -，当时上式可以解出,，并得到最优决策面  神经网络算法流程图如下：    图1.1 神经网络算法流程图  总结：神经网络有很强的非线性拟合能力们可以映射任何复杂的非线性关系，且学习规则简单，易于实现，具有分类准确性高，并行分布处理能力强，分布存储及学习能力强对噪声有较强的鲁棒性和容错能力。支持向量机具有可以提高泛化性能，解决高维问题及非线性问题，避免神经网络结构选择和局部极小点问题的优点。两个算法各有其优点，也有缺陷，暂时还不能确定选择哪个算法对本文的数据进行处理，因此本文会比较两个算法，选出更加适合本文中的数据的算法，并根据计算过程中的缺陷和不足对算法进行改进。  具体的算法流程图如下：    图1.2 算法流程图（总）  其中的步骤分为如下六步：  1、在Internet网络中将报文捕获，存储在本地，然后用Python编写程序将这些DNS报文的内容解析出来，并将DNS中可以利用的字段录入数据库中。  2、解析出来的DNS数据分为两个部分，一部分的DNS数据作为训练集，另一部分留作测试集。先将字段利用PCA算法进行降维计算，然后将数据库的存储表中不能直接计算的字段先量化，并将需要融合的字段进行处理量化，降维流程图如下：    图1.3降维算法流程图  3、用神经网络算法和SVM算法分别进行计算分类，得到较好的参数，并得到结果。  4、再利用剩下的DNS报文作为测试集，计算测试结果的正确性，比较两个算法的结果，观察哪一个算法更为适用于本文的数据中。    图1.4分类器流程图  5、得到更加适合的算法后，再重复流程图中的内容，用不同的训练集和测试集训练算法，并找出算法的纰漏，对算法进行改进和优化，使系统的识别结果更加精确。  6、验证结果有效性。本文模型调试好后，再次取一部分测试集，对DNS报文进行检测分类，并将结果进行检验，计算其准确率、召回率，并与同类模型进行比较。 |

|  |
| --- |
| 六、论文的创新点或实用性 |
| 创新性：  1、对报文的所有内容进行特征提取。  本文设计针对DNS攻击报文的特征的算法，特征的选取均是针对报文的内容的提取，目前存在的攻击报文识别并没有将报文中所有的字段利用上，本文将首次对DNS报文的各个维度的特征进行分析。  2、PCA算法和机器学习中的神经网络算法和SVM算法综合利用。  由于报文可以利用的字段过多，需要利用PCA等降维方式，找出最重要的维度和关联性较强的维度，将维度压缩，然后利用机器学习汇中的神经网络算法和SVM算法对样本报文进行分类处理。将目前较为新的降维算法和目前较热的机器学习算法综合利用。  实用性：  本文针对目前最常见的fast-flux攻击进行分析，找到这种攻击的报文的特点，并设计系统滤除攻击报文。由于很多僵尸网络的攻击针对本地缓存，因此在客户端即攻击的最末端再加上一层保护，也是很有必要的。 |
| 七、研究计划进度和预期成果 |
| 研究计划进度：  2016.10~2016.10 对项目进行需求分析，提出初步的解决方案。  2016.11~2016.11 确定各项系统功能的实现方法，完成开题报告。  2016.12~2017.3 对DNS报文数据的预处理及分析过程进行深入理解与学习  2017.4~2017.5 对数据进行特征提取，并着手算法设计  2017.6~2017.7 详细设计、系统编码与实现  2017.8~2017.9 进行测试，完成整个系统的搭建，项目结束。  2017.10~2017.11 完成毕业论文初稿  2017.12~2018.2 论文修改、定稿  2018.3~2018.3 毕业答辩  预期达到的结果：  1、系统可以通过机器学习的算法实现DNS报文数据的特征提取和分析；  2、系统在不影响正常报文的情况下，识别存在异常行为的DNS报文并阻止其进一步攻击；  3、毕业论文达到合格及以上要求。 |

|  |
| --- |
| 八、导师意见  （请对项目的意义、具体内容、创新点和取得预期成果的可能性等进行评价） |
| 本论文针对DNS fast-flux攻击特征进行研究，采取降维、机器学习等方法，提出一种基于DNS fast-flux的异常行为检测 模型，实现一套在客户端防范fast-flux攻击的识别系统，具备一定实用性。论文目标清楚，采取技术路线、实验方法适当，具备一定创新性，同意开题。  导师签字： |
| 九、研究生部审核意见 |
| 审核老师签字： |