一种恶意域名检测技术的研究与实现

国家计算机网络应急技术处理协调中心江苏分中心 蔡 冰 马 旸 王林汝

摘 要： 研究了一种基于域名解析数据的恶意域名检测关键技术，针对传统恶意域名检测系统的不足，将“域名解析时间突发性”作为一项重要指标引入至系统的检测模式中，并结合大数据分析技术，实现了一套恶意域名检测的原型系统。通过使用真实域名解析数据进行一系列测试，验证了算法的可用性与高效性。

关键词： 域名解析； 恶意域名； 大数据分析

0 前言

我国互联网市场规模和用户体量正处在一个高速增长的阶段，伴随着信息化水平与互联网技术的迅猛发展，来自网络安全方面的威胁也层出不穷，特别是僵尸、木马、蠕虫等恶意程序给我们带来了极大的网络安全威胁，网络环境治理工作面临着日益严峻的挑战。《江苏省互联网网络安全报告》中指出，2014年江苏省内被境内外主机通过僵尸木马控制的事件有189 917 016起，涉及受控IP地址661 639个，黑客通过僵尸木马等恶意程序窃取个人隐私、实施钓鱼欺骗、控制个人终端，严重危害公共互联网安全。

DNS（域名系统）作为互联网重要的基础设施，它主要负责完成IP地址与域名之间的相互转换。然而，由于DNS的开放性，黑客常会构造众多恶意域名用于实施网络攻击或肉鸡控制[1]，而这些攻击、控制记录都会存于DNS解析数据中，通过分析挖掘海量DNS解析数据，从中发现其中的恶意域名是近期网络安全的热点，也是本文的主要研究内容。

1 DNS解析数据方法的引入

相对于传统恶意域名检测使用的恶意程序逆向、DPI（深度报文检测）技术，利用DNS解析数据方法具有独特的优势[2]，国内外科研机构均开展了一系列从DNS解析数据中挖掘恶意域名的探索[3-5]。相对于传统的程序逆向、DPI等基于内容的检测技术，基于DNS数据的恶意域名检测技术具有部署简单、覆盖范围广、匹配精确等独特优势。

本文在国内外学者相关研究的基础上，引入“域名访问活跃度分布特征”这一评判指标，综合考虑域名长度、域名字符特征等因素，提出一套有效的恶意域名检测方法；结合大数据分析技术将理论化的检测方法进行了实现，设计实现了基于DNS数据的恶意域名检测关键技术的原型系统；以某省某年5月20日1.7亿条真实DNS解析记录为原始数据，验证了恶意域名检测关键技术的正确性与有效性。

2 恶意域名检测原型系统设计

2.1 系统架构

本文基于恶意域名检测的关键技术构建了一套原型系统，系统主要分为两大模块：数据采集模块和恶意域名检测模块。

1）数据采集模块。系统在设计与验证过程中使用的DNS数据均来自于某省运营商的全量DNS镜像数据，通过架设DNS采集服务器、镜像交换机以及光电转换等设备实现DNS请求解析数据的采集汇聚，最后将数据回传至本地大数据中心。数据采集模块系统架构如图1所示。

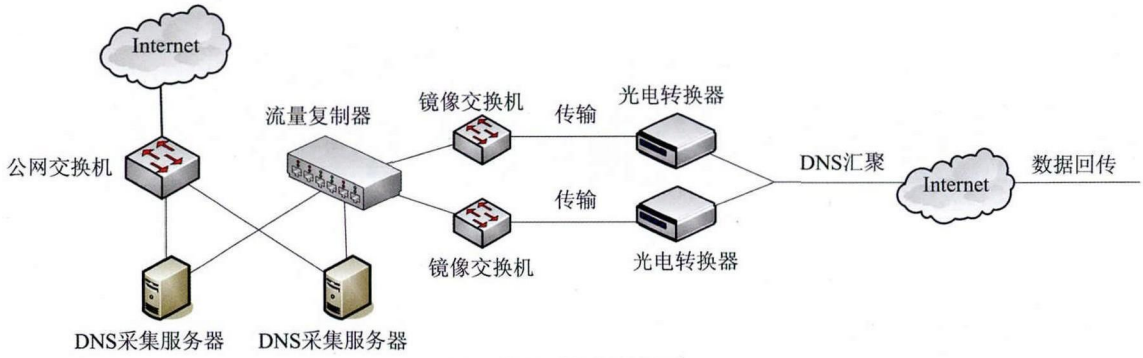

图 1 数据采集模块结构

2）恶意域名检测模块。本地大数据中心接收到回传来的DNS数据后，按照DNS协议字段对海量DNS解析数据进行解析、清洗、入库，再根据系统设计的检测原理进行运算，生成经过判别的恶意域名结果。恶意域名检测模块结构如图2所示。

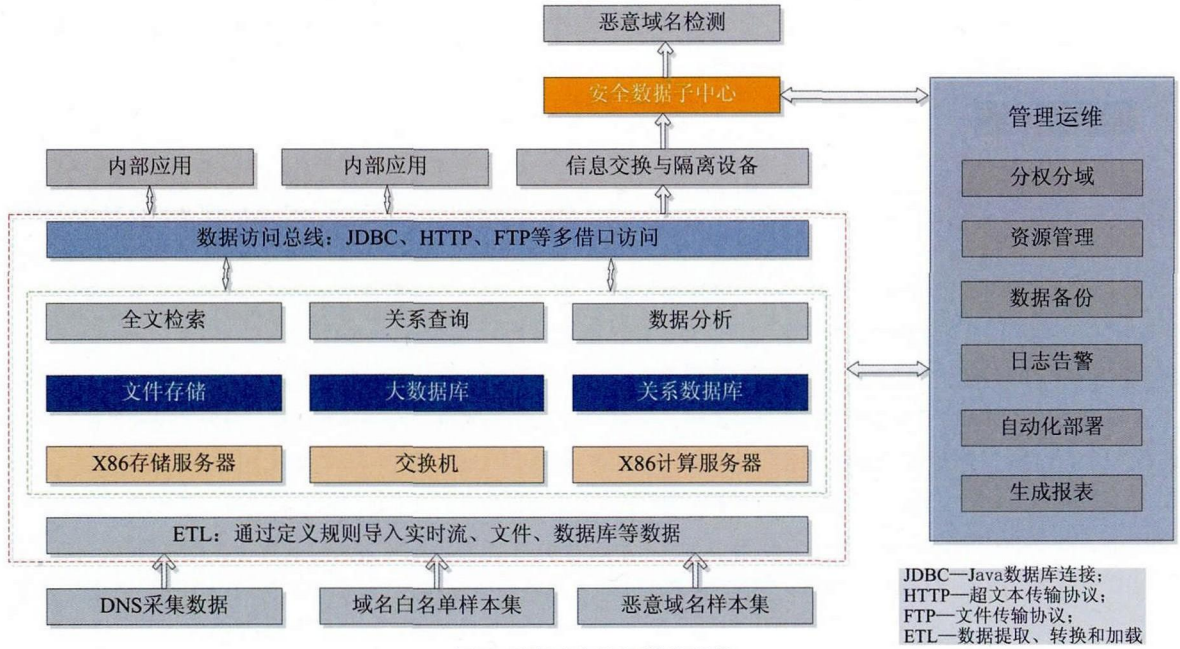

图 2 恶意域名检测模块结构

2.2 检测模式

通过长期对大量恶意域名样本进行特征分析，本文提出了判别恶意域名三个重要模式：

模式一：域名字符长度大于 x 个字符。为了便于用户的访问，正常域名一般不会过长而且具有较为明确的含义；但恶意域名一般不会被用户主动访问（即通过浏览器输入网站地址的方式访问），其为了避免与合法域名产生冲突，通常会由黑客编制特定算法生成。我们经过对大量恶意域名进行长度特征统计，将系统的第一个判别模式设置为长度大于 x 的域名。

模式二：域名由数字和字母混杂无序组成。通过长期对域名样本特征统计发现：正常域名大部分由纯字母构成，即使同时包括字母和数字字符，其组织规则也比较规整，数字和字母通常分开排列，且具有较明确的含义，如163.com、zhibo8.com等；但恶意域名具有生成随机性，很大一部分恶意域名会出现字符和数字混杂的情况，比如已经被证实为恶意域名的vipdn123.blackapplehost.com、exkn0md6fh.qsdgi.co、spykit.110mb.com等。

模式三：域名解析具有时间上的突发性。域名在短时间内被集中访问，而在其他时间内被请求解析次数极少，即我们认为该域名的解析具有时间上的突发性。出于隐藏自身的考虑，大部分恶意域名通常存活时间只有几分钟到几小时，被请求解

析次数分布非常不均匀。恶意域名被黑客控制者所控制大部分时间是处于未激活状态，其解析数量几乎为0，只有当黑客发起攻击指令，“肉鸡”才会产生大量恶意域名的DNS解析请求。

根据模式三的理论，我们建立了相应的数学模型。一般情况下恶意域名的活跃时间约为半小时，也即半小时后该域名通常就被弃用。假设当前待分析域名为 y，设置10 min为一个时间单位对该域名的活跃度分布进行统计，一天分为144个时间单位，即从 T_1 到 T_{144}，用 $C(y,T_i)$ 表示 T_i 时间段内域名 y 被请求解析的次数，在计算 $C(y,T_i)$ 时考虑了 T_{i-1}，T_i，T_{i+1} 三个时间单位的解析次数，用 $\sum c(y,T_i)$ 表示域名 y 一天内总共被请求解析的次数。最后用 $D(y)$ 来表示域名 y 在短时间内的活跃程度。模式三所对应的数学公式如下：

$$D(y)=\max(D(y,T_i))=\max(\mathrm{sum}(C(y,T_{i-1})+C(y,T_i)+C(y,T_{i+1})))/\sum_{k=1}^{144}\sum c(y,T_k),$$

$$i\in[1,144]。$$

根据定义可知，当 $D(y)$ 取值越大表明域名 y 在短时间内活跃程度越高，成为恶意域名的几率也就越大。

2.3 检测流程

根据2.2节中3项检测模式，我们设计并实现了基于DNS数据的恶意域名检测系统，系统工作流程见图3。

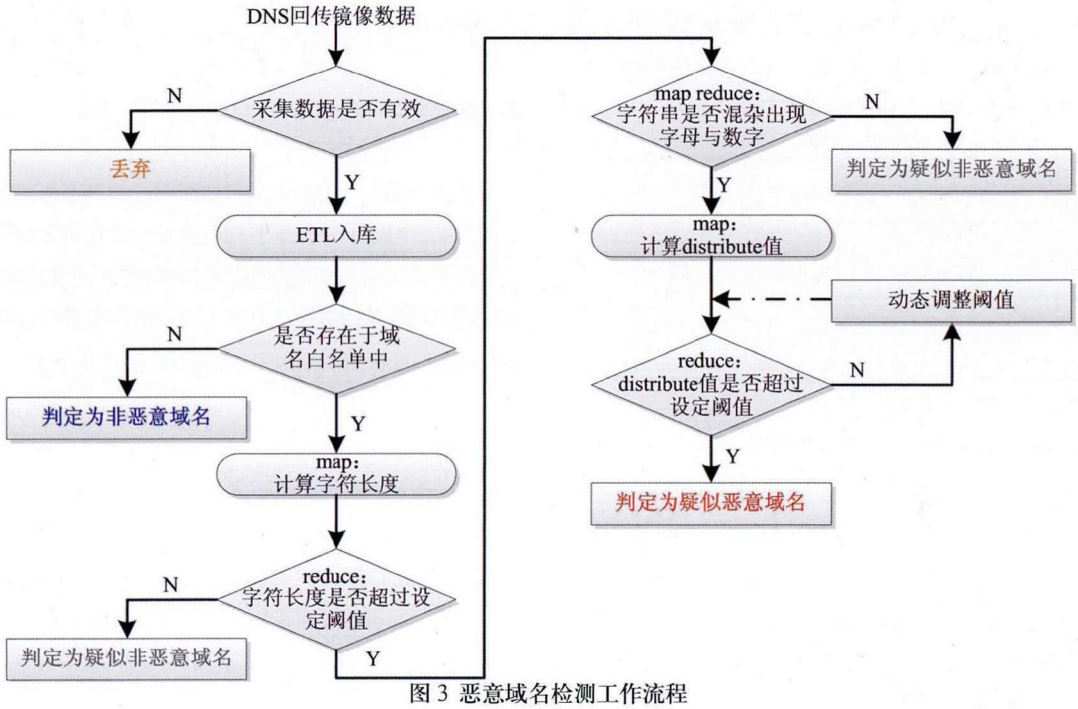

图3 恶意域名检测工作流程

1）对采集的运营商DNS数据进行有效性判断，剔除格式错误或缺项记录，格式无误的记录ETL入库至大数据分析平台；

2）由于全量DNS数据规模庞大，首先根据收集的域名白名单样本集对DNS数据进行过滤，去掉对已知合法域名的请求解析记录，减小后续运算数据量；

3）依据2.2节中模式一进行恶意域名的第一步筛选，得到长度超过 x 字符的域名集合；

4）依据2.2节中模式二进行恶意域名的第二步筛选，通过正则表达式匹配的方式，找出字符串中混杂出现字母和数字的域名集合；

5）最后依据2.2节中模式三进行恶意域名的最后一步筛选，生成最终的恶意域名。

3 检测结果验证与分析

3.1 样本数据集

1）恶意域名样本共计5 000条，主要用于与系统分析结果相比对，验证系统的有效性。该样本主要有三个来源：第一部分是从专业网站（如Malware domain list[6]、Quttera）下载的恶意域名库；第二部分是从搜集到的流行僵尸程序样本，如Conficker，Strom和Kraken等生成的恶意域名；第三部分来自知名安全厂商提供的恶意域名列表。

2）白名单样本共计250 000条，主要用于提高系统检测性能。该样本主要有两个来源，一是采用了Alex排名前10 000的域名以及它们的子域名，二是来自知名安全厂商提供的已知合

法域名库。

3）DNS 解析记录数据 1.7 亿条，我们以某省某年 5 月 20 日真实 DNS 解析记录为原始数据作为本系统分析的数据源，并预先确认其中存有 1 100 个恶意域名，借此统计该系统检测的漏报率。

实验使用的大数据分析集群的硬件配置为：15 台框架式物理服务器，单台服务器配置为 2 颗 AMD 6320 单 CPU8 核心，主频≥ 2.8 GHz，48 GB 内存，8 块 1 TB 的 SATA 硬盘。

3.2 系统测试结果

3.2.1 测试一：仅使用模式一和模式二进行筛选

测试一仅考虑域名长度和域名字符构成因素，而不考虑域名解析突发性的特征。拟定的恶意域名字符构成正则表达式为：.[0–9]*.[a–zA–Z]*.[0–9]*. 或 .[a–zA–Z]*.[0–9]*.[a–zA–Z]*.，其中“*”表示匹配前面的子表达式任意次，“.”表示匹配除“\r\n”之外的任何单个字符。测试一的实验结果如表 1 所示。

表 1 测试一结果

域名字符长度阈值	准确率 /%	误报率 /%	漏报率 /%
8	26.2	73.8	4.7
10	27.6	72.4	7.2
12	31.3	68.7	12.7
14	30.4	69.6	19.9
16	30.5	69.5	27.6

3.2.2 测试二：仅使用模式三进行筛选

参照测试一，仅采用模式三进行恶意域名的筛选。测试过程中，选取了几组不同的 $D(y)$ 阈值作为恶意域名判别过滤条件，并分别统计了准确率、误报率和错误率。不同 $D(y)$ 阈值下的测试结果如表 2 所示。

表 2 测试二结果

$D(y)$阈值	准确率 /%	误报率 /%	漏报率 /%	处理时间 /h
0.8	80.1	19.9	19.1	≈17.5
0.85	83.5	16.5	23.3	
0.9	87.4	12.6	27.9	
0.95	88.1	11.9	28.2	

3.2.3 测试三：综合使用三个模式的进行筛选

首先根据域名白名单对测试样本（假设为 B）进行过滤得到 B1，接着对 B1 按照测试一的方式进行第一轮筛选得到 B2，再次对 B2 按照测试二的方式计算其中各域名的 $D(y)$ 值，根据设定的 $D(y)$ 阈值筛选得到最终结果集 B3。表 3 给出了当设置域名长度阈值为 12、$D(y)$ 阈值为 0.9 时的实验结果。

表 3 测试三结果

域名特征	准确率 /%	误报率 /%	漏报率 /%	处理时间 /h
域名长度超过 12 字符 $D(y)>0.9$	87	13	30.3	≈2

3.3 测试结论

通过上述三组测试我们得出结论如下：

1）测试一仅通过 DNS 静态特征（检测模式一与模式二）进行恶意域名的检测，测试结果误报率过高，算法基本不具备可用性。然而，静态特征适合作为粗粒度的检测条件，可用于快速从测试样本中提出疑似度较高的恶意域名。

2）测试二引入域名的突发性特征检测后（检测模式三），系统准确率明显提升，误报率较低，但由于部分恶意域名在全天的活跃度整体不高且较为离散，导致仅具备模式三的检测漏报率较高。

3）从准确率上看测试三与测试二几乎相当，但由于增添了静态特征匹配与白名单机制，系统处理性能与可用性均得到了大幅提升。

4 结论

本文在提出三项恶意域名检测模式的基础上，结合大数据分析技术，构建了一种基于 DNS 数据的恶意域名检测关键技术的原型系统。为了验证检测技术的有效性，利用真实的 DNS 解析数据对系统进行了功能测试，测试结果表明经过优化后恶意域名检测性能得到了较大幅度的提升，检出率可达到 85% 以上。

参考文献：

[1] OLLMANN G. Botnet communication topologies[EB/OL]. [2015–07–02]. http://www.docin.com/p–909121310.html.

[2] PERDISCI R, CORONA I, DAGON D, et al. Detecting malicious flux service networks through passive analysis of recursive DNS traces[C] // Proceedings of 25th Annual Computer Society Security Applications Conference(ACSAC), Honolulu, HI, USA 2009: 311–320.

[3] PASSERINI E, PALEARI R, MARTIGNONI L. Detecting and monitoring fast–flux service networks[C]// Proceedings of the 5th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA). Paris France, 2008: 186–206.

[4] SANDEEP Y, ASHWATH K.K. REDDY. Detecting algorithmically generated malicious domain names[EB/OL]. [2015–07–02]. http://www.docin.com/p–726881165.html.

[5] Ricardo, Jose Carlos. Identifying botnet using anomaly detection techniques applied to DNS traffic. [EB/OL]. [2015–07–02]. http://www.docin.com/p–193846443.html.

[6] MALWARE DOMAIN LIST. Malware domain list[EB/OL]. [2015–07–02]. http://www.malwaredomainlist.com/mdl.php. ◆