**北京航空航天大学计算机学院**

**硕士学位论文文献综述**

**论文题目**：恶意域名检测技术研究

**专 业**：网络与信息安全

**研究方向**：网络安全

**研 究 生**：王文博

**学 号**：ZY1506221

**指导教师**：兰雨晴 周渊

**北京航空航天大学计算机学院**

2016年12月13日目 录

1 概述 1

2 恶意域名使用现状分析 1

3 发展概况 3

3.1 被动DNS介绍 3

3.2 佐治亚理工学院研究概况 4

3.3 其他研究概况 9

4 主要成果 16

4.1 Nominum 16

4.2 微步在线 17

4.3 360网络安全研究实验室 17

5 主要参考文献 17

摘 要

恶意域名是指当前存在恶意行为或者被恶意使用的域名，近些年来利用恶意域名实施恶意行为的情况越来越多，钓鱼网站、大部分的僵尸网络以及DDoS攻击等都属于这一范畴，相应随之产生了诸多切实有效的对抗与防御措施。

本文简要介绍了恶意域名使用现状，并针对性地详细阐述对应的常用检测方法与思路。分别叙述了几年来国内外学校与研究机构的研究成果以及商业机构的技术运用成果，对恶意域名的检测领域有一个综合性的考量与介绍。

**关键词：****恶意域名；域名系统；网络钓鱼；域名生成算法；僵尸网络；**

**Abstract**

Malicious domain name refers to the current existence of malicious acts or malicious use of the domain name, the use of malicious domain name in recent years the implementation of malicious acts more and more, phishing sites, most of the botnets and DDoS attacks belong to this category, the corresponding Followed by a number of effective confrontation and defense measures.

This paper introduces the current situation of malicious domain names, and expounds the corresponding detection methods and ideas in detail. Respectively, over the past few years, domestic and foreign schools and research institutions and commercial organizations, the results of the use of technology, the detection of malicious domain names have a comprehensive consideration and description.

**Key words：Domain name system; phishing; domain name generation algorithm; botnet；**

**恶意域名检测技术**

# 概述

IP地址是由IP协议提供的数字型统一地址标识，作为一种逻辑地址来定义一台设备在网络之中的位置，网络设备逐渐增多IP地址的记忆困难显现出来，保罗·莫卡派乔斯 (Paul Mockapetris) 在1983年的第882和在南加州大学里资讯科学研究院所提出的883号因特网标准草案中提出DNS的架构，提议将其改进为分布式和动态的数据库域名系统，也就是我们今天所用的域名系统的雏形。[1] 从1985年Symbolics公司注册的第一个.com域名[2]到如今仅中国域名总数增长至3698万个[3]，域名产业飞速发展，随之而来的安全问题也越来越多的暴露出来。作为早期互联网协议，DNS从设计之初就建立在互信模型的基础之上，是一个完全开放的协作体系，其存在的许多缺陷也使得它成为僵尸网络，钓鱼网站等恶意网络行为当中的重要一环。随着互联网应用的不断普及和网民数量的不断增加，网页种植木马技术不断发展，恶意网站给网民带来的安全威胁正在迅速增加。为应对这种恶意网络行为，传统的方法是通过域名黑名单的方式来阻止恶意域名的活动。然而，随着一些新的网络技术的应用，恶意域名的使用变得越来越灵活，大量涌现的许多短生命周期的恶意域名，快速变更的域名和IP地址对应关系使得传统方式难以应对[4]。对于恶意域名检测技术的研究主要分为逆向工程、信誉系统、机器学习三类。逆向工程具有误报率低、召回率高的优点，但是耗时耗力、对攻击反应不及时；信誉系统具有检测速度快、误报率低的优点，但是召回率较高，更新滞后；机器学习方法具有高效、便捷、实时性高的优点，相对前两者精度略有差距。

# 恶意域名使用现状分析

近年来，已经有一些学者企业机构等对恶意域名进行了相关研究。Bilge等[5]把涉及恶意活动的域名滥用行为定义为恶意域名，CNCERT/CC在报告[6]中重点关注涉及网络钓鱼网页挂马僵尸网络的恶意域名，下文将对应用进行具体介绍。

域名阴影（Domain Shadowing）是指利用劫持的合法域名账户在合法域名之下创建大量的子域名。Angler作为当前市场上最强大的钓鱼工具包，于2015年3月份首先推出了这项技术[7]。其原理如图1-1所示，攻击者一般会使用渗透技术（钓鱼网站或者键盘记录木马等）或者社会工程方法获取合法的域名登记者账户，一次性在这些域名下创建大量的子域名来满足恶意的目的。通常这些子域名都进行重定向到攻击者准备好的恶意网站（例如钓鱼网站、广告网站），这些网站充满了挂马与陷阱。而这些危险都隐藏在一个合法的域名之下，导致难以检测和对抗。

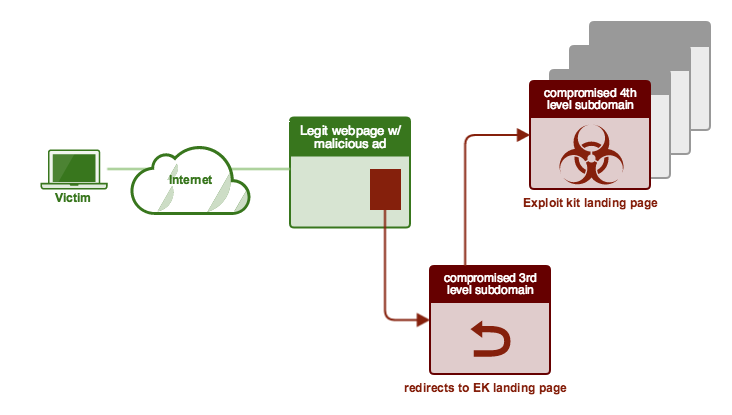


图1-1 域名阴影技术原理

DGA（Domain generation algorithms）是域名生成算法，被大量的恶意软件家族所使用，用以建立受感染主机与C&C服务器（command and control servers）的联系。传统僵尸网络使用固定IP或者域名与C&C服务器建立连接，隐蔽性很差，极易被发现。后来出现的例如Nugache[8]，Storm[9]，Waledac[10]，Zeus[11]等基于P2P的僵尸网络虽然具有较好的鲁棒性与稳定性，但实现难度和维护成本较高。如今大部分活跃的僵尸网络都采用了DGA，依赖于集中的C&C服务器，相比于前两者具有简单易行，兼顾稳定性与隐蔽性的优点。

速变服务网络(Fast-Flux Service Network,FFSN)[12]也是一种恶意软件隐藏自己恶意行为的一种常见技术。Fast-Fux不仅在僵尸网络方面有所应用，在被广泛使用于钓鱼网站和垃圾邮件。Fast-Flux为一个域名配置多个IP地址，DNS的解析结果会不断的变化，两次访问同一个域名，可能会得到不同的结果，可以有效的避免IP地址的封锁。利用此特征，僵尸网络控制者可以将其控制的肉鸡中服务能力比较强、具有公有ＩＰ的肉鸡作为代理，其他一些服务能力比较弱的主机通过与这些代理通信，代理将通信重定向到后面真正的控制者，完成控制者与肉鸡的通信过程。僵尸网络控制者通过频繁的更换域名到代理ＩＰ的映射，从代理网络中剔除不可用的以及服务能力较弱的代理，提高网络的健壮性和可用性。[13]

DDoS（Distributed denial-of-service）是指分布式拒绝服务攻击，在利用流量来实施的DDoS攻击中，只要有可以利用来进行放大数据量的协议，都有可能被恶意使用。正常的DNS查询是从原IP地址向DNS服务器（递归或者权威），大小相对固定（70字节左右），也就是攻击成本相对固定，DNS返回数据由于请求域名和类型的不同，数据大小从几百到几千字节（查询[www.baidu.com.的返回数据为302](http://www.baidu.com.的返回数据为302)字节），放大了四倍以上。由于利用A记录或者Cname记录放大效果并不十分明显，Akamai研究人员在2014年发现了利用TXT记录来进行的DNS放大攻击，攻击者使用名为DNS Flooder的工具，从guessinfosys.com获得TXT记录，攻击峰值高达4.3Gbps[14]。

钓鱼网站（phishing page）一直以来都是一个难以规避的网络问题，同时他也是一种社会工程学的攻击方式[15]。通常攻击者对恶意页面进行伪装，使得页面看起来像是银行网站或是其他可以获取关键隐私信息的网站，受害者往往由于受到邮件或者短信的欺骗，通过其中的链接导向到钓鱼网站，或者由于误植域名导向到钓鱼网站。而受害者对于网站的真伪缺少足够的判断和辨识的能力，导致银行账户密码等隐私信息被攻击者窃取。

# 发展概况

## 被动DNS介绍

被动DNS（PassiveDNS）数据是网络安全领域最为常用的资源之一，该数据收集技术由Florian Weimer于2004年提出[17]，主要目的是将DNS流量转换为易于访问的格式。递归域名服务器会响应其接收到的来自其它域名服务器的请求，对响应进行记录并将日志数据复制到中央数据库当中，因此记录这些数据就掌握了DNS解析的历史动态。Zdrnja等人首先说明了如何利用被动DNS从域名中获得安全信息[16]，2008年Plonka等人提出了Treetop[18]，它可以弹性地管理逐渐增长的被动DNS数据，并在同时关联域和网络属性。他们的聚簇区域是基于不同的种类的网络。Treetop依据是否符合各种DNS RFC标准以及解析结果来区分DNS流量并提供部分安全信息。

## 佐治亚理工学院研究概况

佐治亚理工学院的M.Antonakakis、P.Roberto、W.Lee等人在2008年开始了对DNS数据的研究，先后对DNS缓存投毒、域名信誉系统、DGA、僵尸网络等方向都做出了很高的贡献。在2010年建立的Notos[19]，是一个动态的综合性的信誉系统，首次提出了针对域名的信誉系统，利用被动DNS数据来输出信誉分数，而于此之前主要针对IP的信誉系统完全不同。Notos使用了网络和地区的特征，通过配置信息、使用情况和域名管理情况等，能够学习良性和恶性的域名分别是如何工作的，并对每一个新域名计算一个信誉得分。对于一个域名，如果它与恶意活动(例如僵尸网络、垃圾邮件、恶意软件传播等等)有关，就给他赋予一个低的信誉值，图3-1是Notos系统的整体流程。

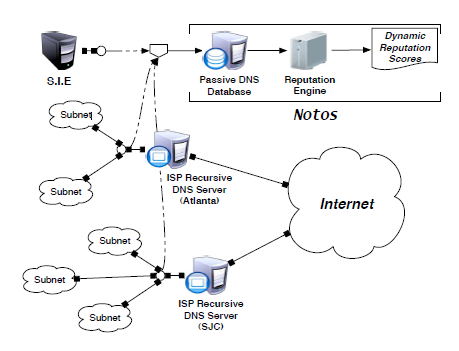


图3-1 Notos系统的整体流程

首先利用被动DNS数据构建三组特征：

1. 基于网络的特征：第一组的统计特征是从RHIPs的集合中提取的。计算如下特征：与d历史相关的IP地址的总数量、它地理位置的多样性、它们所在的不同的自治系统的数量等等。
2. 基于域的特征：第二组特征是从RHDNs集合提取的。计算在RHDNs里域名的平均长度、不同TLD的个数、不同字符出现的频率等等。
3. 基于证据的特征：最后一组特征包括与d相关的不同恶意软件样本的数量、与d曾经指向的IP相关的恶意软件样本的数量等等。

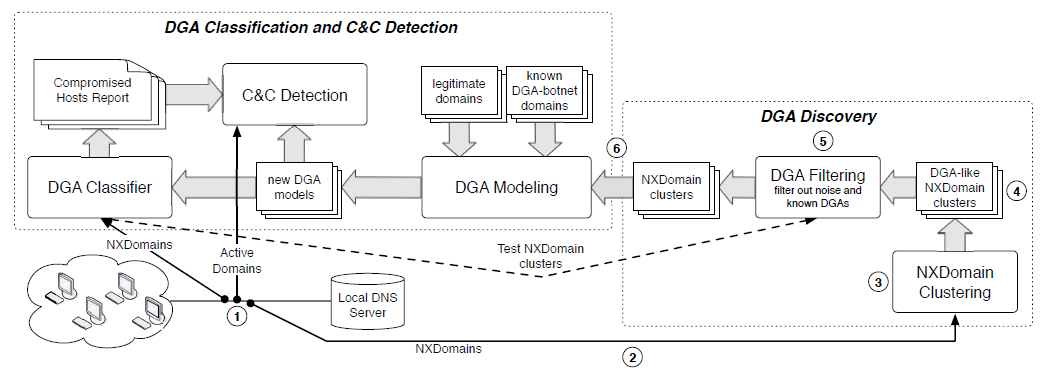
Notos的信誉引擎有两个运行模式：离线训练模式和在线分类模式。在离线模式下，Notos使用在知识库中收集到的数据来训练信誉引擎，知识库即一组已知的恶意和合法的域名及其相关的IP地址。在之后的在线模式中，对于每一个新域名d，Notos询问信誉引擎从而为d计算一个信誉值。动态信誉评分系统的基础是从成功解析的域名A记录中获得的历史或“被动的”信息。作者使用了来自两个ISP的采集节点的DNS流量，一个位于美国东海岸(亚特兰大)，另一个位于美国西海岸(圣荷西)。另外他们也汇总了SIE项目中不同网络的DNS流量。数据库收集到了从2009年7月19号至2009年9月24号这68天的解析记录共27377461条。结果Notos可以以96.8%的精度和0.38%的误报率发现恶意域名，并且它比黑名单方法更快。

2011年Manos Antonakakis等人构建了一个叫做Kopis的恶意域名监测系统[20]，可以通过对DNS查询解析模式的分析得到恶意域名，与EXPOSURE和Notos这些依赖本地递归DNS服务器的系统相比，Kopis使用的是上级DNS数据。在此基础上他们在2012年又提出了一个新颖的检测系统Pleiades[21]，首先使用了不存在域名（NXDOMAIN）响应。NXDOMAIN是指像域名服务器提出解析请求，但是无法解析得到对应IP。对于使用DGA的被控主机大多数查询都会返回一个NXDomain，而同一僵尸网络控制下(使用相同的DGA算法)的被控主机会产生有类似特征的NXDomain的流量。Pleiades聚类和分类算法的结合，充分利用了机器学习的优势，将有着相似字符特征和相似访问特征的域名聚集在一起。分类算法用来将这些生成好的聚簇分配到已知的DGA模型中去。如果一个聚簇不能被分到已知的DGA中去，那么意味着可能出现了新的DGA变种或DGA家族。

图3-2是Pleiades的整体流程。DGA发现模块分析了未成功的DNS解析流量，它部署在DNS服务器的下游。在一定时间段内网络产生的所有NXDomains都会被收集在内。接着，收集到的NXDomains会根据以下两个相似准则分别被聚类：(1)域名字符串所具有的相似的统计特征(例如相似的长度、随机性和有关字符的频率分布等)；(2)域名被一组相同或相近的IP访问。对NXDomain聚类的主要目的是将那些使用同一种域名生成算法的主机和域名聚类出来。由于这个聚类过程是无监督的，所以聚类出来的某些NXDomain簇里可能包含那些偶然错误的域名(例如由于拼写或者配置错误导致的NXDomains)。因此需要对这些数据进行过滤。作者使用有监督的DGA分类器去修整这些聚类簇，修正的对象包括已经发现并建模的DGA产生的域名和那些与合法的域名相近的域名。DGA发现模块最终的输出是NXDomains的聚簇集，其中的每一个集合都代表了已知或者未知DGA产生的域名。每当发现一个新的DGA，就使用监督学习方法为这样的域名建立一个模型，该模型用来描述新DGA产生的域名“长什么样”。为此建立了两种不同的统计模型：(1)一个为肉鸡产生的一组NXDomains赋予DGA标签(如DGA-Conficker.C)的多类统计分类器；(2)基于隐马尔科夫模型判断查询过的可能由一个DGA产生的活跃的单一C&C域名的类型。DGA分类模块的工作过程如下。与DGA发现模块相似，作者监测DNS递归服务器中由每个主机产生的NXDomains流量。给定一个主机产生的NXDomains的子集，然后提取与其字符串有关的一系列统计特征。接着将这些特征作为特征向量传入分类器函数，分类器会输出这些NXDomains是否由一个已知的DGA产生。如果一个主机产生的NXDomains被贴上了相关的DGA标签，那么这个主机也极有可能被相关的僵尸网络所控制。一旦获得了那些感染主机的列表，就可以进行更深一步的检测。之前所有步骤都是围绕无效域名NXDomains展开的，下一步则把注意力集中到这些感染主机访问的活跃域名上。其目标是确定哪些由DGA算法生成的域名最后解析成了IP地址，即识别僵尸网络的C&C服务器。为了实现这一目标，作者将感染主机访问过的所有可疑活跃域名都收集起来。接着对这些域名输入之前训练好的隐马尔科夫模型中，由它来决定单一活跃域名是由已知DGA产生的或是未知DGA产生的。使用隐马尔科夫模型而不是分类器做判断的原因是需要对单一域名进行检测。DGA分类器不适合单一域名的检测，因为它根据一个感染主机产生的一组无效域名进而判断这组无效域名是哪种DGA产生的。



图3-2 Pleiades的整体流程



作者使用Bobax, Sinowal, Conficker-A, Conficker-B,Conficker-C和Murofet产生的NXDomains来引导分类器。在两种模式中测试分类器。第一种模式使用Conficker的一个“超类”，它由Conficker-A, Conficker-B和Conficker-C的相同数目的样本组成。另一种模式则将Conficker的每个变种作为不同的类别看待。从每个类的域名中，作者随机选取了大小为α的3000个集合。其使用的α值有2、5、10和30。这是建立不同的训练集的过程，目的就是通过实际证明哪个α值可以给出DGA模型之间的最佳的分割。

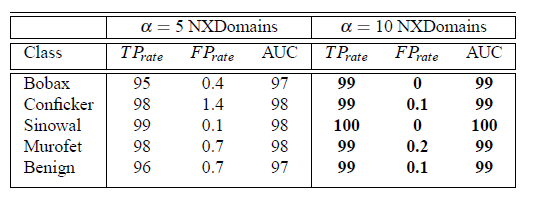


表3-1 不同下使用折交叉验证的检测结果(单位 %)



Pleiades从2010年11月的第一天就开始对NXDomains流量进行聚类。作者使用已知的DGA作为正例和一组Alexa域名作为反例来引导DGA建模过程。通过检查NXDomains与从恶意程序库中提取到的NXDomains的重叠关系来发现恶意程序家族。另外他们也在威胁情报公司的帮助下手动地检查了聚簇，检测出每个DGA变种有着平均32个感染主机，这些主机横跨全州的ISP网络。通过十几个月的实验，我们证明了Pleiades可以达到一个很高的精确度。此外，Pleiades部署在大型ISP网络下的这15个月来，它可以发现6个属于已知恶意程序家族的DGA和6个之前从未报出过的DGA。

Pleiades有一些局限。例如，一旦发现一个新的DGA，Pleiades可以很准确地为它建立统计模型，它可以知道这种DGA产生的域名“长什么样”，但它不能通过学习重现它的域名生成算法。因此，Pleiades会产生一定程度的假正和假负。但是上表的数据表明，Pleiades可以建立一个很准确的DGA分类器模型，当α=10时假正和假负都很低。C&C检测模块可以判断单一活跃域名的DGA种类，在大多数情况下表现很好。但是有一些情况下基于HMM的分类有些问题。作者认为这样的原因是HMM只考虑了域名的单一字符序列。总体来说，Pleiades聚类和分类算法的结合，充分利用了机器学习的优势，将有着相似字符特征和相似访问特征的域名聚集在一起，分类算法用来将这些生成好的聚簇分配到已知的DGA模型中去，是这个领域非常重要的一篇文章。

## 其他研究概况

除开佐治亚理工学院的这些人，其他地区的研究者和组织也对这个领域做出了极大的贡献。Perdisci 等提出 FluxBuster 系统[24], 这是一个专门针对速变域名检测的系统，将域名的 IP 变迁情况引入特征集, 共 9 组 13 个特 征, 采用聚类算法来识别速变域名。除了针对某一种域名的检测系统，更多的是具有广泛适用性的系统。

2011年L.Bilge等人建立了EXPOSURE系统[23]，一个检测多种恶意域名的系统。该系统从DNS数据中分别基于时间、基于DNS响应、基于生存时间值（TTL）、基于域名提取了这4类共计15种特征，使用J48决策树训练分类器。相比于Notos，Exposure有着更完善的特征选取，也弥补了无法检测一个IP地址只被恶意使用一次的恶意域名。相比于之前文章都只能在DNS数据中找到特定种类的恶意域名，EXPOSURE对恶意域名的检测更加广泛。

2013年Terry Nelms，Roberto Perdisci等人构建的ExecScent[25]是一个旨在从真实的企业网络流量中挖掘新的、从未出现过的C&C域名的系统，同时ExecScent也是第一个使用自适应C&C流量模型的系统。ExecScent从已知的C&C通信样本中自动地学习控制协议模板(CPT)，并且这些CPT会匹配它们所部署的网络流量。ExecScent构建的这种自适应模板从部署模板的网络流量中学习，这种“自适应”的方法使得ExecScent在保持一个很高检出率的同时极大地降低了误报率。

ExecScent自动地寻找不同恶意样本的C&C协议间的共同的特点，接着将这些共性编码进CPT集合中。每个模板都标有恶意程序家族的名称或者与该C&C流量相关的犯罪组织(如果有的话)。一旦将CPT部署在网络的边缘，任何与该模板匹配的HTTP(S)流量就会被认为是C&C流量。与该流量相关的域名就会被标记为C&C域名，并且会归于恶意程序家族或者与该CPT关联的组织。图3-3展示了ExecScent生成和标记CPT的整体过程。

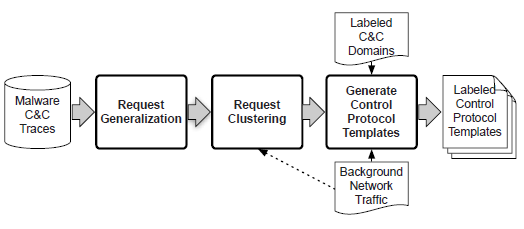


图3-3 ExecScent系统概述

给定一个大的恶意软件生成的网络痕迹，首先重构每个恶意样本的HTTP请求。接着，进行一个“请求泛化”的过程，这里将请求的一些参数(如URL参数值)替换为它们的类型和长度。当恶意程序的请求被聚类后，我们进行模板学习过程，在这里我们推导出CPT。本质上讲，一个CPT高度概括了聚在一起的HTTP请求，并且记录了一系列重要的特征如URL结构、请求头的集合、每个恶意软件访问过的IP地址等等。此外，这些模板与恶意程序家族标签一一关联。在真正部署模板前，作者先把CPT放在应该部署到的网络流量中观察一段时间。特别是对于模板的每一个组件(如泛化的URL路径、user-agent字符串、请求头集合等等)，计算各个组件在部署网络中出现的频率。在背景流量中“活跃”的那些组件会在该网络中得到一个低的“匹配信任”。另一方面，在流量中那些不经常(甚至是从来没)出现的组件会得到较高的信任。部署后，如果一个HTTP请求被CPT以很高的相似性和特异性所匹配，那么它就会被标记为C&C请求。这就是说，一个请求与CPT描述得很接近并且匹配的CPT的组件在特定的部署网络中有着很高的特异性(即不经常出现)。

2016年B.Rahbarinia创新性的提出了一种基于行为的系统Segugio[26]，Segugio在大的ISP网络中通过追踪被恶意软件感染主机的DNS请求行为来高效的发现新增的malware-control域名。相比于Notos和EXPOSURE，前两者建立的都是domain-IP映射关系模型（使用域名字符串的特征、域名承载的恶意内容等信息）而没有利用本地DNS服务器下游的主机请求行为，Segugio通过监测ISP网络用户的DNS请求行为，重在精确的追踪新增的“malware-only”域名。相比于Kopis，他的做法和本文有相似性（Kopis用请求者散度、请求者画像等信息），但Kopis利用权威或TLD服务器的数据，这种数据难以获得（需要与大的DNS区域运营商紧密合作）。Segugio不用关心顶级域名，通过监测本地ISP流量（在ISP使用者和他们的本地DNS解析器之间的DNS流量）。因此Segugio可以依靠ISP网络权限独立开发，不需要与外部的DNS运营商合作。

D.Plohmann，F.Fkie等人针对DGA做了大量细致的工作[27]，他们对43种DGA恶意软件家族和变种进行一个综合性的研究，针对DGA提出一个分类学方法，并用它对所研究的DGA进行分类与比较。并重现了这些算法，预先计算所有可能的AGD，覆盖了大部分已知的活跃DGA，以过去8年总计18millionDGA域名的注册状态，来证实预计算得到的域名确实是是可靠的。对于botmaster的域名注册策略也提出了见解。

DGA作为一种随机算法，输出为域名，作者将算法输入称为种子（例如数字常量、当前时间、Tiwwter动态等），按照种子产生类型以及算法类型，可以对DGA进行分类。如果这个种子与时间有关，称之为TD（time-dependent，时间相关），反之，称为TI（time-independent，时间无关），如果种子可以估计（例如日期），称为D（Determinism，可估计），反之（例如欧洲央行每天外汇参考利率），称为N（Non-determinism，不可估计）。域名产生模式分别有A（Arithmetic，算法类）、W（Wordlist，单词表类）、H（Hashing，哈希类）、P（Permutation，置换类）四种。进行排列组合理论上有16类DGA，实际上只出现了TDD-A, TID-A,TDD-W , TDD-H, TDN-A , TID-P 这六种类型。

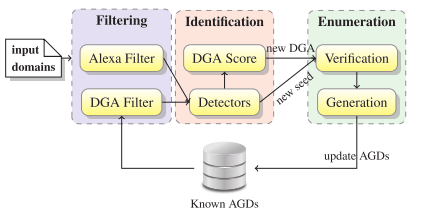


图3-4 DGA收集过程

图3-4为作者的DGA域名收集过程，实际工作中首先通过恶意软件分析报告和blog，定义了最初的22个DGA家族。然后利用Alexa top-ranked10000的域名和已知AGD（由DGA算法产生的域名）进行过滤。接下来是识别的过程，构建探测器用来检测一个给定域名是否符合已知DGA的输出，捕捉产生域名的最大最小长度，DGA字母表，已知TLD等字符特征。如果域名模式相同，标为使用新种子的已知DGA；如果不一致或者域名数量不足，通过计算一系列数值，例如n-gram，熵，长度等，来判定是否是新的DGA种类。当检测出来是一个可能的新DGA算法，人工进行逆向工程来验证。

国内也有很多机构活跃在恶意域名的检测领域，中国科学院信息工程研究所有大量与此相关的文章。张洋等人基于多元属性特征的恶意域名研究[28]针对的是域名域名的伪装特点和跳变特点，针对性从多个角度地提取一些特征进行恶意域名检测。 如“taobao.xxx.com”，可以从域名词法角度提取属性特征，也可以通过其网络属性来进一步丰富属性特征，如生存时间值(Time-To-Live，TTL)。表3-2与表3-3是文章所使用的11个词法特征和9个网络特征：

、

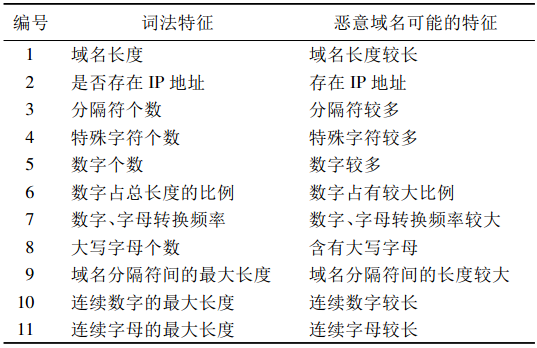


表3-2 词法特征



表3-3 网络特征

文章使用随机森林分类器对恶意域名和正常域名进行分类。随机森林分类器具有诸多优势: 能够处理高维数据，能够处理多种格式的数据，能够处理缺失的特征，能够平衡误差，不会出现过拟合的现象等。鉴于此，随机森林分类器非常适合对域名进行分类。随机森林分类器作为基于机器学习的一种集成学习方法，结合了多个决策树的分类效果，最终通过投票方式选出得票最多的类别作为最终的分类。实验结果表明，该方法的准确率、召回率99.8%，具有较好的检测效果。

张永斌等人认为相同周期内产生的僵尸网络域名大多具有相同字符特征，被感染主机有相同行为特征，提出了他们的一个检测算法[29]。整个检测算法分为：数据预处理、失效域名聚类分析、新域名聚类分析、恶意域名提取4个处理过程。其中数据处理过程主要是判断一个解析成功的域名是否是新域名，并将网络中主机请求的新域名及失效域名信息进行保存，以便后续分析。失效域名聚类分析过程主要是通过请求失效域名的主机IP地址信息对失效域名进行聚类分析，提取 出可疑失效域名集合、潜在感染主机集合。新域名聚类分析过程主要是通过新域名解析返回的IP地址对新域名进行聚类分析，利用聚类结果将请求主机划分多个请求组。恶意域名提取过程主要是通过失效域名聚类结果，对请求每个新域名集合的主机组进行分析，判断组内主机在域名请求行为上是否具有组行为特征，提取出最终的恶意域名、感染主机、C&C服务器IP地址集合，并对分析结果进行评估。

国家互联网计算机网络应急技术处理协调中心张雪松等人提出了对算法生成恶意域名的实时检测[30]。图3-5是算法的处理流程，主要包括下面几部分：数据采集及预处理、已知算法生成恶意域名的解析及访问关系构建、新增域名与已知域名的关联分析、未知域名的跟踪分析。

数据采集与预处理主要是通过镜像DNS流量，实时过滤并提取新增域名，利用域名白名单机制降低待处理的数据量。系统从DNS流量中提取域名，保存到域名数据库，并通过一段时间的数据收集建立域名的检测基线，依靠基线提取新增域名作为系统分析对象；收集并整理已公布和确认的算法生成恶意域名，作为关联分析的基础。将已确认恶意域名按照域名结构及解析内容进行分组，在内存中建立域名分组与解析IP集合分组与访问客户端集合的对应关系，用于后续与新增域名间的关联分析；新增域名与已知域名分组进行关联后，如确定域名属于某一分组，输出并更新域名分组信息，否则对新增域名持续跟踪，收集域名的解析及访问数据，按照周期分析域名的活跃情况，判定域名是否为算法生成的恶意域名。

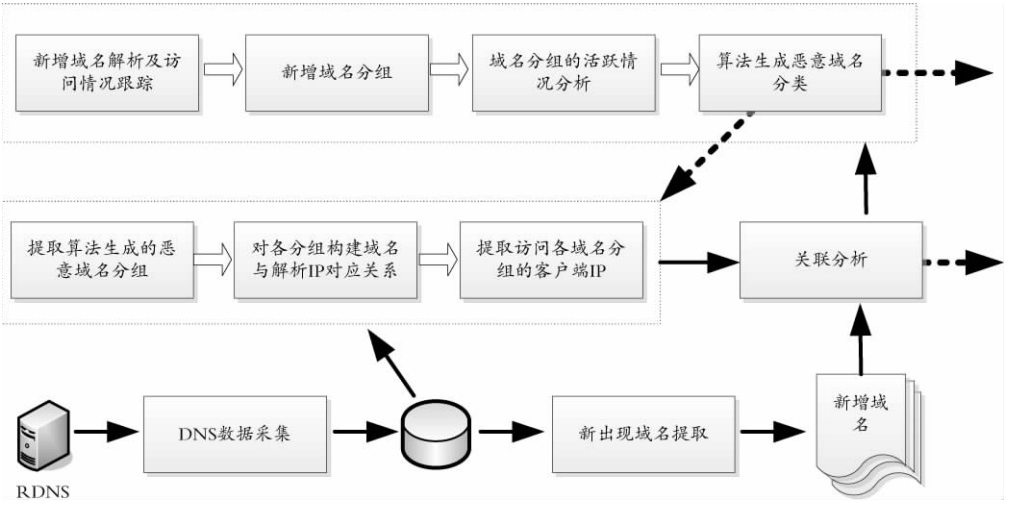


图3-5 域名实时检测流程

除了这些机构，一些高校对此也有所研究，东南大学张维维等人针对黑名单在维护和更新上存在开销大和及时性差，且攻击者常常使用算法自动生成大量的随机域名来躲避检测的不足以及实时检测开销过大的缺陷，设计了轻量级的检测算法来快速锁定监测目标，以便有针对性地使用更为复杂和更为准确的检测算法[33]。轻量级算法需要在有限的系统资源和计算时间内，尽可能多地检测出可疑域名因此，算法设计优先考虑空间开销和计算复杂度，而检测精度可以由更为复杂和更为准确的后续算法去保证。

文章依据最小的语言学单位—词素，设计启发式字符串切割算法快速切分域名，并在二层域名标签聚类的基础上，通过统计域名所含词素的比重、均长和频率分布熵等特征测度，应用有监督的机器学习方法检测恶意服务使用的非法域名。 为验证算法的可行性，作者基于统一的标准域名集，比较词素特征与已有n元组频率分布以及单词特征的检测能力。实验结果表明：词素特征能够有效地刻画域名字面的语言学特征，与n元组频率分布特征相比，可以提高检测准确率，降低假阳性，有效抵挡攻击者借助事前相应特征统计的逃避策略以及借助字典或Kwyjibo工具的随机域名生成策略；与单词特征相比，在保证检测准确率的同时，较小的词素集可以保证算法具有较低的计算复杂度和存储开销。最后，实际应用该轻量级算法对中国教育科研网江苏省网边界采集到的域名集进行检测，结果表明：该算法具有较高的检测准确率(87.2%)、较低的内存开销(80.14MB的临时内存,2.71MB的常驻内存开销) 和计算复杂度(运行时间196.1s)。

# 主要成果

在学术领域Notos、Pleiades、Kopis、EXPOURE等一些列经典的系统都已在上文中仔细介绍过了，这一章节的重点放在国内外工程与商业上的应用成果。

## Nominum

Nominum是为网络运营商提供综合型用户、网络和安全解决方案的全球领先提供商[31]。Nominum所建设的N2平台每天处理的DNS查询量超过一万亿次，实现利用DNS数据的应用的快速开发与无缝集成。在海量数据的支持下，始终活跃在抗击网络攻击的最前线，同时提供着最权威的安全报告，对当前流行的、危害高的网络威胁（例如Ddos、随机子域名攻击等）都有着最为细致的分析。图4-1是他们的DNS数据分析系统。

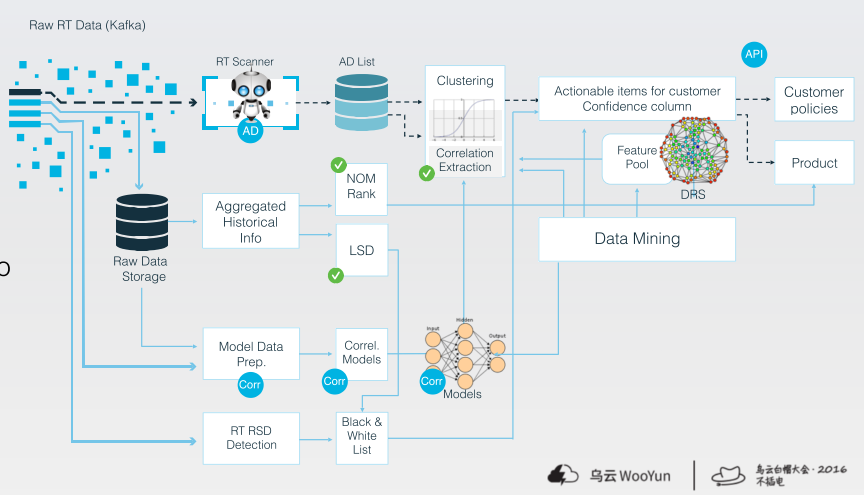


图4-1 NominumDNS数据分析系统

## 微步在线

微步在线（ThreatBook）是一家从事专业威胁情报的公司，所发布的威胁分析平台VirusBook（www.virusbook.cn），也是国内首款综合性威胁情报分析平台。随着定向攻击及APT的日益泛滥，业界清醒的认识到：单纯的防御方式很难消除面临的关键风险，安全检测和响应的重要性重新被发现，作为贯穿检测－定位－决策－行动全过程的威胁分析已成为当今的热点。现阶段安全分析师所使用的分析平台主要是国外的站点，如VirusTotal、DomanTools、PassiveTotal及一系列的开源情报站点。但是这些站点还存在着一些问题：首先，这些站点大多只提供了分析所需要的某一方面的信息，并不能完全覆盖整个分析过程，导致分析师需要到多个站点进行查询，并手动进行关联分析，这样的工作无疑是枯燥、低效的，严重影响了分析师能力的发挥；其次由于网络的问题，某些重要网站往往不能正常使用，使工作难以进行。而微步的威胁分析平台做到一个站点完成鉴别、定性、溯源、追踪等多重任务，弥补了国内市场的不足。

## 360网络安全研究实验室

这里需要介绍一下360网络安全实验室所建立的一个威胁情报项目[32]，公布了所有的检测数据并且做到每天更新，主要分为以下四个部分：

* 针对全自动攻击工具Exploit Kit的行为检测；
* 对20个DGA家族和超过170个种子的实时追踪；
* 对任一个IP、域名或者MD5值的恶意软件关联；
* 当下流行的恶意代码扫描。

# 主要参考文献

1. https://zh.wikipedia.org/wiki/%E4%BF%9D%E7%BD%97%C2%B7%E8%8E%AB%E5%8D%A1%E6%B4%BE%E4%B9%94%E6%96%AF
2. 25 Years Later， First Registered Domain Name Changes Hands，https://techcrunch.com/2009/08/27/25-years-later-first-registered-domain-name-changes-hands/
3. 第38次中国互联网络发展状况统计报告. CNNIC，2016.
4. 赵雷. 基于DNS的恶意域名识别系统的设计与开发[D].山东大学,2013.
5. Kirda Leyla,Bilge Engin.EXPOSURE:Finding Malicious Domains Usi ng Passive DNS Analysis. NDSS . 2011
6. CNCERT互联网安全威胁报告.2016.
7. Nick Biasini.Threat Spotlight: Angler Lurking in the Domain Shadows. 2015.
8. S. Stover, D. Dittrich, J. Hernandez, and S. Diet- rich. Analysis of the storm and nugache trojans: P2P is here. In USENIX ;login:, vol. 32, no. 6, De- cember 2007.
9. Wikipedia. The storm botnet. http://en. wikipedia.org/wiki/Storm\_botnet, 2010.
10. J.Williams. What we know (and learned) from the waledac takedown. http://tinyurl.com/ 7apnn9b, 2010.
11. abuse.ch. ZeuS Gets More Sophisticated Us- ing P2P Techniques. http://www.abuse.ch/ ?p=3499, 2011.
12. Riden J. Know your enemy: fast-flux service net- works [EB/OL]. 2008.http://www.honeynet.org/papers/ff
13. T. Holz, C. Gorecki, K. Rieck, and F. Freiling. Measuring and detecting fast-flux service networks. In Proceed- ings of NDSS, 2008.
14. Attackers are increasingly leveraging large Domain Name System (DNS) TXT records in an effort to amplify the impact of their distributed denial-of-service (DDoS) attacks, Akamai's Prolexic Security Engineering and Research Team (PLXsert) warned on Tuesday,http://www.securityweek.com/large-dns-text-records-used-amplify-ddos-attacks-akamai
15. T. Moore and R. Clayton. An empirical analysis of the cur- rent state of phishing attack and defence. In Proceedings of the Sixth Workshop on the Economics of Information Secu- rity, 2007.
16. B. Zdrnja, N. Brownlee, and D. Wessels. Passive mon- itoring of DNS anomalies. In Proceedings of DIMVA Conference, 2007.
17. F. Weimer. Passive DNS replication. In Proceedings of FIRST Conference on Computer Security Incident, Hand ling, Singapore, 2005.
18. D. Plonka and P. Barford. Context-aware clustering of DNS query traffic. In Proceedings of the 8th IMC, Vou- liagmeni, Greece, 2008. ACM.
19. Antonakakis, M., Perdisci, R., Dagon, D., Lee, W., & Feamster, N. (2010). Building a Dynamic Reputation System for DNS. USENIX Security’10: Proceedings of the 19th USENIX Conference on Security, 1–17.
20. Antonakakis, M., Perdisci, R., Lee, W., Ii, N. V., & Dagon, D. (2011). Kopis:Detecting Malware Domains at the Upper DNS Hierarchy. USENIX Security Symposium., 11, 1–16.
21. Antonakakis, M., & Perdisci, R. (2012). From throw-away traffic to bots: detecting the rise of DGA-based malware. Proceedings of the 21st USENIX Security Symposium, 16.
22. Antonakakis, M., Perdisci, R., Lee, W., Ii, N. V., & Dagon, D. (2011). Kopis:Detecting Malware Domains at the Upper DNS Hierarchy. USENIX Security Symposium., 11, 1–16.
23. Bilge, L., Kirda, E., Kruegel, C., Balduzzi, M., & Antipolis, S. (2011). EXPOSURE : Finding Malicious Domains Using Passive DNS Analysis. Ndss, 1–17.
24. Perdisci R, Corona I, Giacinto G. Early detection of malicious flux networks via large-scale passive DNS traffic analysis. IEEE Transactions on Dependable and Secure Computing, 2012, 9(5): 714–726
25. Nelms, T., Perdisci, R., & Ahamad, M. (2013). ExecScent: Mining for New C&C Domains in Live Networks with Adaptive Control Protocol Templates. Proceedings of 22nd USENIX Security Symposium, 589–604.
26. Rahbarinia, B. (2016). Segugio:Efficient and Accurate Behavior-Based Tracking of Malware-Control Domains in Large ISP Networks, 19(2).
27. Plohmann, D., Fkie, F., Yakdan, K., Klatt, M., Bader, J., Gerhards-padilla, E., … Bader, J. (2016). A Comprehensive Measurement Study of Domain Generating Malware. USENIX Security Symposium.
28. 张洋,柳厅文,沙泓州,时金桥. 基于多元属性特征的恶意域名检测[J]. 计算机应用,2016,04:941-944+984.
29. 张永斌,陆寅,张艳宁. 基于组行为特征的恶意域名检测[J]. 计算机科学,2013,08:146-148+185.
30. 张雪松,徐小琳,李青山. 算法生成恶意域名的实时检测[J]. 现代电信科技,2013,07:3-8.
31. http://www.nominum.com/
32. http://data.netlab.360.com/
33. 张维维,龚俭,刘茜,刘尚东,胡晓艳. 基于词素特征的轻量级域名检测算法[J]. 软件学报,2016,09:2348-2364.