一种高效的恶意域名检测框架

崔甲， 施蕾， 李娟， 刘照辉， 姚原岗
（中国信息安全测评中心，北京 100089）

摘 要：由于域名系统缺乏足够的安全机制，常作为黑客发动网络攻击的重要行动基础设施. 因此如何快速准确地发现并阻断潜在的恶意域名及对应 IP 是防范未知网络攻击的重要手段和研究热点. 讨论了恶意域名检测领域已有研究成果及其优缺点，提出了一种结合三种域名检测技术的新型恶意域名检测框架 MDDF，结合实验结果讨论了该框架具备更好的检测效率及较好的完备性.

关键词：恶意域名检测；被动 DNS；机器学习
中图分类号：TN915.08 **文献标志码**：A **文章编号**：1001-0645(2019)01-0064-04
DOI：10.15918/j.tbit1001-0645.2019.01.011

An Effective Malicious Domain Detection Framework

CUI Jia， SHI Lei， LI Juan， LIU Zhao-hui， YAO Yuan-gang
(China Information Technology Security Evaluation Center, Beijing 100089, China)

Abstract: Since the lack of sufficient security mechanism, domain system has become the main operational infrastructure for hackers to launch cyber attacks. Therefore, how to discover and block the potential malicious domain and the corresponding IP address quickly and precisely have become an important measure and a hot research direction in preventing unknown cyber attacks area. Based on deep investigation of the achievements in malicious domain detection fields, combining three different malicious domain detecting methods, a novel malicious domain detection framework (MDDF) was proposed. According to the experimental results, MDDF can improve the detection efficiency and provide a preferable completeness.

Key words: malicious domain detection; passive domain name system; machine learning

当前全球网络空间的国家级博弈与对抗日趋激烈，以关键信息基础设施作为主要攻击目标的安全事件频发（例如 2016 年的乌克兰停电事件[1]）. 在非协作网络环境下，传统以 IP 追溯(trace back)技术定位攻击者的方法已无法作为指认攻击者身份的直接证据，因此如何溯源真正的攻击者及幕后组织成为难题. 美国国防部高级研究计划局(DARPA)早在 2011 年就提出以革命性方法研究威胁溯源归因的“网络基因组计划”[2]，之后又于 2016 年提出“增强归因计划”[3]，两个计划都是研究以恶意代码分析、行动基础设施分析以及攻击组织画像为主的溯源分析关键技术，并且它们均已成熟应用于美国近年来针对中国等国家发布的 APT 报告中，例如 APT1[4]、APT30[5]、APT10[6]、CAMERASHY[7]等. 大量 APT 报告中都包括针对域名系统 DNS 数据的检测分析，并结合 Whois 等基础信息库对攻击者的溯源分析.

作为互联网核心服务的域名系统（domain name system，DNS），其功能是将域名和 IP 进行相互映射. 由于在设计上缺乏安全验证机制，常作为黑客发动网络攻击重要行动基础设施. 例如，为逃避检测、阻断和追踪而采用 Fast-Flux[8]技术和随机域名生成算法 DGA[9]. 国内外安全界已认识到分析 DNS 数据在发现、防范、预警外部网络威胁等方面的重要价值.

收稿日期：2017-07-30
基金项目：国家自然科学基金资助项目(U1536118)
作者简介：崔甲(1981—)，男，博士，E-mail：cuij@itsec.gov.cn.

1　MDDF 框架

在充分调研和深入分析已有恶意域名检测研究成果的基础上,综合各类恶意域名检测方法的优缺点,本文中提出了一个新型的恶意域名检测框架(malicious domain detection framework,MDDF). 该框架通过综合各检测技术的优势,弥补了各自缺点,最终综合每种检测方法的评分,给出最终的域名信誉度评分,能够客观描述域名的恶意程度. 该框架适合部署于大型网络 ISP 的汇聚口,如图 1 所示.

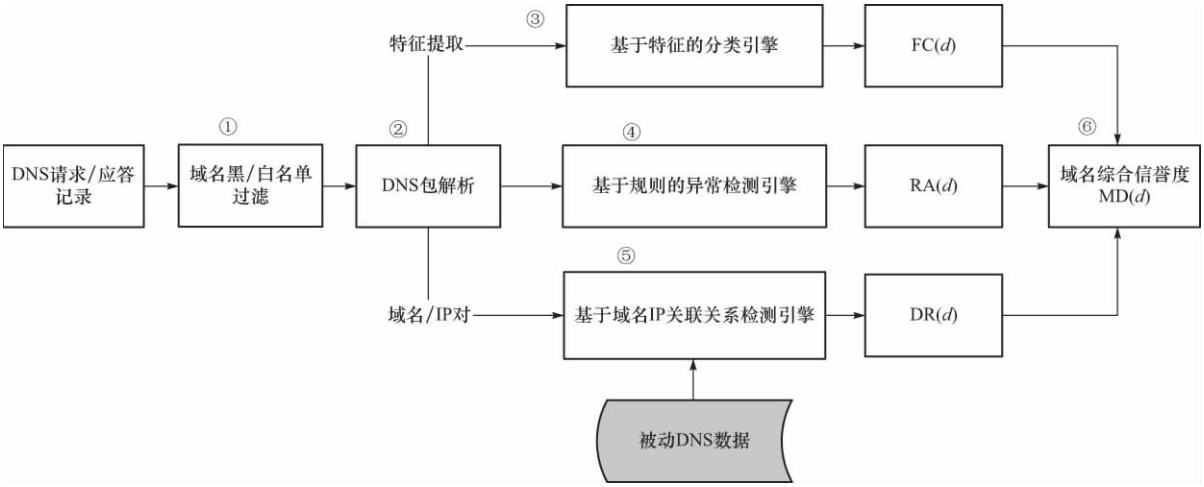

图 1　MDDF 恶意域名检测框架

Fig. 1　Malicious domain detection framework

MDDF 框架包括六部分.

① 黑/白域名过滤器. 过滤的本质是对接入的 DNS 请求/应答报文进行标记,排除包含在域名白名单对应的 DNS 报文,告警域名黑名单中对应的 DNS 报文,然后仅分析那些“灰色”域名的属性,目的是减少真实分析的数据量. 域名黑白名单的获取来源于开源威胁情报网站或权威网络安全公司网站,如表 1 所示.

表 1　域名黑白名单来源

Tab. 1　Blacklist and Whitelist source

黑名单	白名单
domains. com	Alexa. com top 20 000
zeustracker. abuse. ch	root. cn top 500
malwaredomainlist. com	Google top 200
wepawet. cs. ucsb. edu	safeweb. norton. com
phishtank. com	Google Safe Browsing
safeweb. norton. com	siteadvisor. com
www. threatminer. com	dmoz. org

② DNS 记录解析器. 依据 RFC 1035 文档正确解析 DNS 报文中各个字段标识,以满足后端 3 个检测分析引擎相应的内容需求. 经过 DNS 记录解析器的 DNS 流量保存为半结构化 json 结构分别输入 3 个检测引擎,每个检测引擎根据需求进行域名分析.

③ 基于特征分类的检测引擎. 通过提取解析的 DNS 记录的字段特征,生成用于检测的特征向量,并将特征向量输入分类器进行检测,给出相应的域名信誉度打分 FC(d). 表 2 给出了提取的 4 类 DNS 特征.

表 2　基于特征分类的恶意域名检测

Tab. 2　Extracted DNS features for classification

类别	特征说明
域名字符串特征	是否包含知名域名
	是否包含特殊名称
	是否包含钓鱼域名
	域名熵特征
	域名长度
	域名包含 Level 层数
	域名数字与域名长度比
时间特征	时间间隔相似度
	相同时间间隔请求次数
TTL 特征	TTL 所在范围[0,1),[1,10),[10,100),[100,300),[300,900)
	TTL 改变次数
	不同 TTL 值的个数
	NS 记录对应 TTL 平均值
	A 记录对应的 TTL 平均值
应答特征	是否包含静默 IP(LAN IP)
	应答报文对应不同 IP 地址个数
	应答报文 IP 对应的不同国家个数
	应答标志位
	应答报文中应答段的 RR 个数
	应答报文中权威段的 RR 个数

④ 基于规则的异常检测引擎. 该检测引擎主要以DNS记录的字段为主,借鉴IDS[11]和DPI检测技术,针对正常DNS请求应答报文中的字段建立规则模型,凡是不符合该模型的均被认为是异常的,给出相应的域名信誉度打分RA(d). 例如:DNS请求域名的应答IP地址指向诸如127.0.0.1、192.168.0.1的内网地址;DNS请求域名的应答IP地址与DNS服务器IP地址相同;DNS应答中的TTL值过小;DNS载荷中包含加密信息等.

⑤ 基于域名IP关联关系的检测引擎. 该检测引擎只关注域名与IP的对应关系,基于被动DNS数据库中的域名和IP历史对应关系. 首先构建一个域名和IP的对应二分图,若两个域名共享IP地址,则在域名关联关系图中连接两个域名,并在两点连接边上赋权重,权重以共享IP数量为计算单位. 之后通过在该图中基于路径信誉度传播算法对域名进行信誉度DR(d)分析计算.

如图2所示,域名$D_1 \sim D_6$对应IP地址$I_1 \sim I_7$,D_3和D_6共享I_2和I_6,则右图中D_3和D_6边权重为2,D_1和D_5不共享IP,则右图中两点不连接. 假设D_3确定为恶意域名,则与D_3共享IP的域名为D_2和D_6,根据边权重,D_3和D_6关联关系更紧密,因此域名D_6的恶意程度高于D_2.

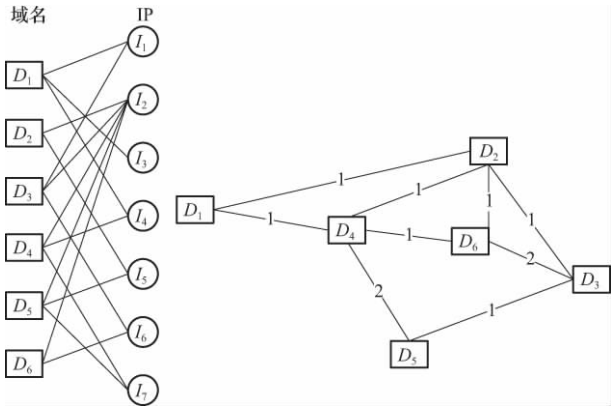

图2 基于域名-IP关联关系的方法

Fig. 2 Domain-IP relationship based method

⑥ 域名信誉度计算器:综合3个检测引擎的信誉度打分FC(d)、RA(d)和DR(d)计算域名的最终信誉度MD(d),计算方法可以采用加权平均等方法获得.

2 实验结果与分析

为了验证MDDF框架检测效率,捕获了本地网络出口7 d的DNS流量,并搭建了一个模拟真实网络流量的实验平台进行重放. 整合了表1的白名单,共包括20 047个二级域名,同时也将黑名单数据进行了清洗和筛选,获得的黑名单信息如表3所示.

表3 域名黑名单信息

Tab. 3 Domain Blacklists Information

恶意域名	Phishing	Conficker	Black-listed	Zenus Botnet	Microsoft Botnet	ThreatMiner
数量	1 181	1 060 500	1 804	190 033	22 036	2 039

对于基于特征的分类检测引擎,随机挑选了4 d的DNS数据用于训练分类器模型,其中包含已经进行标记的已知恶意域名对应的DNS数据. 对于基于域名-IP关联分析的检测引擎,申请了Farsight公司的(http://www.dnsdb.info)的被动DNS查询API,分别查询了白名单和黑名单域名对应的pDNS数据构成pDNS数据库. 基于规则的异常DNS检测使用了国内某安全厂商的IDS产品进行协同检测. 重放7 d的DNS流量进行在线检测,并分别对3个检测引擎检测结果进行评估,最后与MDDF检测结果进行对比.

图3是各检测引擎的实验结果对比(FC:基于特征的分类检测,RA:基于规则的异常检测,DR:基于域名IP关联关系的检测),从结果来看MDDF检测效率最佳. 原因是MDDF框架综合了当前恶意域名检测领域3种最主流的检测方法:基于特征分

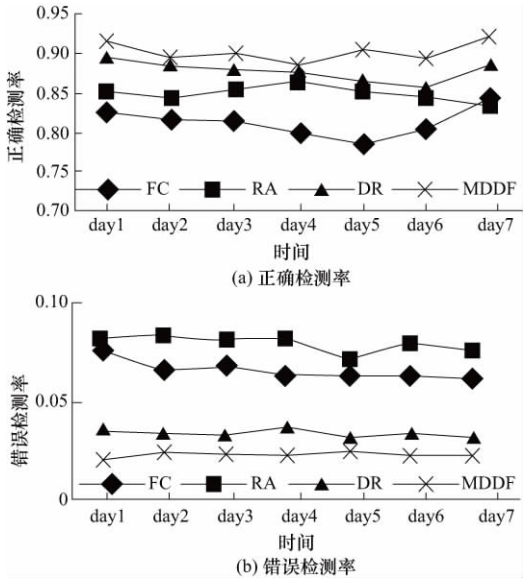

图3 在线检测的实验结果对比

Fig. 3 Online DNS detection experiment results

类的检测方法、基于域名 IP 关联关系的检测方法以及基于规则的异常检测方法,虽然 3 种方法检测方法和技术不同,但目标都是对 DNS 报文及其包含的请求应答域名进行恶意程度分析. MDDF 结合 3 个检测引擎的优势相互补充并同步检测,综合 3 种结果提升恶意域名的检出率,降低误报率.

基于特征分类的检测方法需要从 DNS 报文中提取选择度较高的特征,并需要典型且较完备的样本集进行训练以获得较好的分类效果,但其缺点是如果所获得的样本集与真实测试集有较大区别时则分类的效果不好,需要不断训练更新分类模型,同时攻击者也容易构造 DNS 报文躲避这类检测. 基于域名 IP 关联关系的检测方法则避免了基于特征分类方法的不足,利用域名与 IP 地址之间对应关系对域名进行分析,但如果所检测域名及 IP 地址为攻击者利用的新资源,并未出现在被动 DNS 数据库中,则该方法将失效,同时 pDNS 数据集作为一类高价值数据较难获得. MDDF 中引入基于 DNS 异常的规则检测,是从 DNS 报文中发现不符合正常 DNS 请求应答报文的特征对 DNS 报文进行分析判别,也是一种最直接有效的检测方法,但是所导入的规则需要人工介入不断总结提炼才能加以完善. MDDF 综合了上述 3 种域名检测方法,将他们的优缺点相互补充,从不同角度对 DNS 流量进行分析计算,最终得到一个域名的综合信誉评分. 3 个检测引擎内部还可相互协作,例如基于特征分类的检测方法能够导出特征并生成检测规则,进一步完善基于规则的异常检测方法,而规则产生的误报可以通过基于域名 IP 关联关系的方法进行判断并排除误报.

3　结　论

借助机器学习等高级数据分析技术挖掘 DNS 数据来发现网络中潜在的恶意域名是当前网络安全领域一个热门研究方向,目的是从网络攻击发起的行动性基础设施入手发现攻击者的行动线索并尽早加以阻断并及时进行预警和防护,同时也是网络威胁溯源分析的一个重要支撑. 本文提出的恶意域名检测框架 MDDF 主要针对流量中 DNS 请求应答报文进行检测分析,框架涵盖了 3 类主流的恶意域名检测方法并且将其特点进行相互补充,能够达到较好的恶意域名检测效果.

参考文献:

[1] 安天实验室. 乌克兰停电事件启示录[S]. [S. l.]:中国信息安全,2016.
Antiy Labs. Enlightenment from Ukraine power cut incident[S]. [S. l.]: China Information Security Network, 2016. (in Chinese)

[2] Darpa. Cyber genome program[S]. [S. l.]: DARPA, 2010.

[3] Darpa. Enhanced attribution program[S]. [S. l.]: DARPA,2016.

[4] Mandiant. APT1 exposing one of China's cyber espionage units[M]. Mandiant:[s. n.],2014.

[5] FireEye. APT30 and the mechanics of a long-running cyber espionage operation, how a cyber threat group exploited governments and commercial entities across Southeast Asia and India for over a decade[R]. [S. l.]: FireEye Inc. ,2015.

[6] Anonymous operation cloud hopper[R]. [S. l.]: PWC UK and BAE Systems,2017.

[7] Threat Connect. CAMERASHY closing the aperture on China's unit 78020[R]. [S. l.]: Threat Connect,2015.

[8] Rahbarinia B, Perdisci R, Antonakakis M. Efficient and accurate behavior-based tracking of malware-control domains in large ISP networks[J]. ACM Transactions on Privacy and Security (TOPS),2016,19(2):4.

[9] Craw Ford, Kwyjibo H, Aycock J. Automatic domain name generation[J]. Softw Pract Exper,2008,38(14): 1561-1567.

(责任编辑:刘芳)