•可信计算与信息安全•

DOI:10.15961/j.jsuese.201700632

基于TDRI的多视图关联DNS流量可视分析

陈兴蜀[1,2], 陈敬涵[3], 曾雪梅[2*], 韩珍辉[1], 朱　毅[3], 邵国林[3]

(1.四川大学 网络空间安全学院, 四川 成都 610065; 2.四川大学 网络空间安全研究院, 四川 成都 610065;
3.四川大学 计算机学院, 四川 成都 610065)

摘　要:针对现有DNS流量分析方法受大规模网络中大数据量限制的问题, 及可视分析方法还未应用到DNS流量分析中的现状, 提出了一种TDRI(trend to domain and request information)DNS流量分析模型, 并采用DNS流量分析模型和网络安全及大数据可视分析方法相结合的方式, 设计并实现了基于TDRI DNS流量分析模型的多视图关联DNS流量可视分析系统。首先, 对复杂大规模真实网络中长期、大量DNS流量数据进行观测和描述性分析。然后, 从DNS服务中域名请求者、域名及域名访问3个基本要素的角度抽象并提出一种包含DNS流量特征值时序变化趋势、请求域名及域名访问情况的DNS流量分析模型。最后, 以提出的DNS流量分析模型为指导, 设计了包括数据选择和关联交互视图的DNS流量可视分析系统, 支撑问题分析为驱动的DNS流量数据分析过程。将基于TDRI的多视图关联DNS流量可视分析系统应用于校园网真实环境, 帮助分析者从DNS流量中发现了网络中的恶意访问行为以及针对DNS的恶意行为。实验结果表明, 本文提出的分析方法可提高大规模网络环境下DNS流量分析效率, 分析出DNS流量中表现出的恶意行为, 为DNS安全稳定运行提供了保障。

关键词:DNS; 可视分析; DNS流量分析模型; 大数据

中图分类号:TP393.0　　**文献标志码**:A　　**文章编号**:2096-3246(2018)04-0123-07

Correlative Visual Analytics for DNS Traffic with Multiple Views Based on TDRI

CHEN Xingshu[1,2], *CHEN Jinghan*[3], *ZENG Xuemei*[2*], *HAN Zhenhui*[1], *ZHU Yi*[3], *SHAO Guolin*[3]

(1.College of Cyber Security, Sichuan Univ., Chengdu 610065, China; 2.Cyber Security Research Inst. Sichuan Univ., Chengdu 610065, China; 3.College of Computer Sci., Sichuan Univ., Chengdu 610065, China)

Abstract: In order to solve the problems that the existing DNS traffic analysis is limited by large data in complex large-scale networks, and the current visual analysis is not yet applied to DNS traffic analysis, a DNS traffic analysis model based on trend to domain and request information(TDRI) is proposed. The combined with network security and visual analysis method of big data, a multi view association DNS traffic visual analysis system based on TDRI DNS traffic analysis model is designed and implemented. First, the long-term and massive DNS traffic data of complex large-scale real networks are observed and analyzed. Then, a DNS traffic analysis model that includes DNS traffic eigenvalue time-series trend, request domain, and domain request information is abstracted and presented from three perspectives of requester, domain and request. Finally, based on the proposed DNS flow analysis model, the DNS traffic visual analysis system, which includes data selection and interrelated interactive view, is designed to support the analysis process of DNS traffic data driven by the problem analysis. The multi-view associated DNS traffic visual analysis system based on TDRI is applied to the real environment of campus network, which helps analysts find malicious access behavior in the network from DNS traffic and maliciousbehavior for DNS.The experimental results show that the proposed analysis method can improve the efficiency of DNS traffic analysis in the large-scale network environment and analyze the malicious behavior in the DNS traffic, which provides a guarantee for the safe and stable operation of the campus network DNS.

Key words: DNS; visual analytics; model of DNS traffic analysis; big data

收稿日期:2017 – 08 – 05

基金项目:国家自然科学基金资助项目(61272447); 国家“双创”示范基地之变革性技术国际研发转化平台资助项目(C700011); 四川省重点研发项目资金资助项目(2018G20100); 四川省科技支撑计划资助项目(2016GZ0038); 中央高校基本科研业务费专项资金资助项目(2017SCU11059; 2017SCU11065; SCU2016D009)

作者简介:陈兴蜀(1968—), 女, 教授, 博士生导师, 博士. 研究方向: 云计算、信息安全. E-mail: chenxsh@scu.edu.cn

* 通信联系人 E-mail: zengxm@scu.edu.cn

网络出版时间:2018 – 07 – 09 15 : 28 : 00　　**网络出版地址**: http://kns.cnki.net/kcms/detail/51.1773.TB.20180709.1527.012.html

域名系统(DNS)作为互联网上核心基础设施，是互联网正常通信的重要保障[1]，这一服务的重要性和DNS设计实现本身带来的脆弱性[2]，导致了大量利用DNS系统的网络攻击及针对DNS本身的特定攻击的出现，如：基于DNS的放大攻击、利用DNS的C&C通信、DNS投毒等。使得通过DNS发现恶意网络行为以及监测DNS本身状态具有重要意义。DNS流量数据作为反映DNS服务器状态和使用情况的重要数据，复杂大规模真实网络环境中表现出数据规模巨大，持续迅速增长，层次结构丰富的显著特点，给分析人员高效分析DNS流量带来繁重的认知负担。因此，通过高效的DNS流量分析方法，帮助分析人员快速通过DNS流量数据掌握DNS运行情况，发现网络中的恶意行为，并保障DNS系统的可用性与安全性具有重要意义。

近年来大量研究者针对DNS流量进行了广泛的研究。章思宇[3]通过对恶意软件DNS流量的分析，设计了基于DNS流量的恶意软件检测算法，监测了各类恶意软件。张维维等[4]通过对主干网DNS流量的分析，提出“依赖性”和“使用位置”测度组，以及多分类器模型，地在主干网环境下进行僵尸网络等恶意活动检测。缪晨[5]基于流量分析技术设计实现了DNS DDoS流量检测系统，检测了针对DNS服务器的异常流量。但上述研究在复杂大规模环境下分析效率受数据量的限制。

为了帮助分析人员通过复杂大规模网络数据快速分析网络状况，从“正常状态中”快速准确感知“异常情况”，可视化已成为网络安全研究中的重要方法[6−8]。网络安全可视化研究领域现有研究主要涉及对可视化结构本身的研究和借助多视图合作对网络流量进行可视分析两部分。对可视化结构本身的研究弱化了分析者与可视化工具交互过程的重要性，独立可视化的方法往往不能满足分析者现有的问题分析过程。对于大数据安全可视分析中面临的数据规模大且难以表征的问题[9]，多视图合作分析可帮助分析者通过现有分析过程从网络流量数据中检测并定位网络异常事件。Hao 等[10]提出了以多视图合作为核心展示框架的可视分析工具，提高了分析过程的效率和灵活性。Chen 等[11]设计了针对流量数据的多视图合作在线分析工具，可高效分析识别DDoS等网络攻击事件。赵颖等[12]实现了多视图合作的网络流量时序数据可视分析系统，可较好支撑对常见网络异常的分析。上述研究体现了多视图合作对网络流量异常检测的有效性，但现有相关研究缺乏有针对性地将可视分析方法应用于DNS这一特定核心服务。

作者以DNS流量分析为研究对象，提出了一种基于TDRI(trend to domain and request information)的DNS流量分析模型，该模型基于DNS协议中源IP、目的IP、域名及Rcode等字段，依次对DNS流量特征值不同时间粒度下的时序化趋势分析、请求域名分析、域名访问情况进行分析。并将该模型和可视分析相结合，实现了基于TDRI的多视图关联DNS流量可视分析系统。通过多个协同交互的视图，支撑以问题分析为驱动的DNS流量数据分析过程，帮助分析人员高效分析DNS流量，分析发现DNS流量数据反映出的恶意网络行为及DNS自身面临的攻击。

1 TDRI DNS流量分析模型

通过对DNS流量数据的观察和研究，抽象出图1所示的DNS流量数据分析过程，并提出TDRI DNS流量分析模型。该模型包含DNS流量特征值时序化趋势分析、请求域名分析以及域名访问情况分析3个部分，对DNS服务中域名请求者、请求域名及域名访问情况3个要素进行了描述，从而进行异常流量发现、与异常流量相关的域名跟踪及与域名相关的IP及访问跟踪。

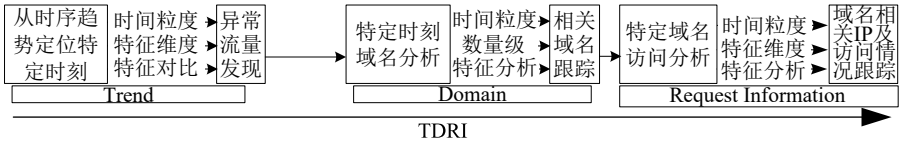

图 1 TDRI DNS流量分析过程

Fig. 1 TDRI DNS traffic analysis process

1.1 从时序变化趋势定位特定时刻

分析特定特征值时序的变化趋势，是TDRI分析模型的关键基础步骤，对定位异于常态的时刻有重要意义，其难点有：1)特征选择，DNS流量数据中哪些特征能反映DNS流量基本状态；2)时间粒度，如何选取适当的时间粒度提高DNS流量分析的准确性；3)异常定位，如何通过相关特征对比定位特定时刻。

作者从两个角度提取时序变化趋势中特定特征值和相应时间粒度：1)DNS流量基本关键特征。DNS流量数据中，访问量、访问者和解析域名通常是分析者关注的3个基本要素，以天为时间粒度的DNS访问量、访问者以及访问域名数量变化趋势展

现一段时间内负载情况变化，帮助定位分析者感兴趣或异常时刻；2）DNS异常流量特征。DNS另一重要特征属性为DNS对域名的解析成功率，解析成功率与DNS访问量时序变化趋势的结合，在相对较小的时间粒度下，如分钟，可帮助定位某些突发事件。如：当出现DNS拒绝服务攻击，域名解析成功率降低但DNS访问量迅速增大[13]。

为分析所选取的DNS请求量、访问者数量和解析域名数量3个基本关键特征两两间的相关性，利用了皮尔逊相关系数计算方法[14]，随机变量X和Y的相关系数计算方式为：

$$r=\frac{\sum_{i=0}^{n}(x_i-\overline{x})(y_i-\overline{y})}{\left(\sum_{i=1}^{n}(x_i-\overline{x})^2\right)^{\frac{1}{2}}\times\left(\sum_{i=1}^{n}(y_i-\overline{y})^2\right)^{\frac{1}{2}}} \tag{1}$$

式中，r为线性相关系数，变量间的正负相关性取决于r的正负，$|r|$大小决定了变量的相关程度，其值越大相关性越高。以天为时间粒度，利用从2016年12月至2017年5月半年的DNS流量数据，计算得到上述半年时间内的DNS请求量、访问者数量和解析域名数量3个基本关键特征两两间的相关性得到结果如表1所示。

表 1　本文所选特征间相关性

Tab. 1　Correlation coefficient of selected features

	请求量及访问者数量	访问者数量及解析域名数量	请求量及解析域名数量
相关系数	0.41	0.93	0.47

以天为时间单位的相关性分析发现，请求量、访问者数量和解析域名数量间表现出一定正相关性。为证实对上述3个特征的选取的有效性，同时选取了域名请求源端口数与上述特征间相关性进行了对比，其结果如表2所示。

表 2　其他特征相关性

Tab. 2　Correlation coefficient comparison of other feature

	请求量及源端口数	访问者数量及源端口数	解析域名数量及源端口数
相关系数	0.40	0.15	0.20

源端口数与各特征值间表现出弱相关性，该结果进一步验证了3个特征选择的有效性。

为分析突发的DNS异常流量，从DNS异常流量特征的角度，将分钟内DNS请求量和域名成功解析率进行对比。成功解析率利用DNS协议中Rcode字段值进行分析如下。

$$P=\frac{s}{T}\times 100\% \tag{2}$$

式中，P为一分钟内DNS成功解析率，s为一分钟内域名成功解析的记录数，T为一分钟内DNS请求记录数。

1.2　域名分析

DNS作为域名解析服务器，无论是恶意软件对DNS的利用还是针对DNS的恶意攻击行为都与域名密切相关[2−3]，通过对异常时间点DNS解析的域名的分析，如：从该时间点解析量大的域名中找出与分析者已有领域知识或认知不符的域名，聚焦可疑域名，帮助分析造成DNS安全问题或引起流量基本属性数据偏离正常值的域名。

1.3　域名访问情况

真正对DNS安全性和可用性产生影响的并非恶意域名本身，恶意访问者以及对域名进行访问的恶意行为，才是异常产生的主体。通过请求域名的IP、各IP对域名的请求次数、IP对域名的查询类型以及IP请求域名的返回状态进行刻画，在域名分析部分锁定可疑域名后，该部分可帮助锁定恶意访问者及其访问行为。

在上述TDRI DNS流量分析模型基础上，设计了DNS流量可视分析系统，下面将介绍具体介绍系统结构设计和多视图关联的DNS流量交互可视分析过程。

2　原型系统设计

相比于直接从海量数据本身获取信息，将数据映射到可视化结构能显著提高分析者对数据的认知能力以及认知的准确性和效率[15]。以2017年4月的数据为例，平均每日产生的DNS应答数据有约1.8亿条，每条数据均包含DNS的消息头部、查询段、应答段授权段和附加段。通过对DNS流量长期的观测分析，本文总结出DNS流量存在数据规模巨大，持续迅速增长，层次结构丰富等特性。针对上述特性，基于TDRI DNS流量分析模型设计了DNS流量可视分析系统。

2.1　系统层次结构设计

DNS流量可视分析系统系统架构如图2所示。该系统包含数据存储、数据处理、可视分析3个模块。

数据存储模块实现了基于HDFS的DNS历史流量数据存储。DNS流量数据处理模块实现了对海量DNS历史数据的清洗，基于关键字段的数据统计，及特征提取。

可视分析模块首先实现URI与处理后数据表中数据资源间的映射，为数据检索并将数据映射到可视化结构的高效性、准确性和可靠性提供保障。接着基于本文所提出的TDRI DNS流量分析模型，实现了以问题分析为驱动的多视图关联的DNS流量可视分

析。为减轻可视化方式本身给分析者造成的认知负担，采用了利用网络安全数据进行网络监控、异常检测以及特征分析中较为常用的折线图、柱状图及平行坐标轴3种可视化结构[8]，直观展现DNS流量数据的数值、变化趋势和流量特征值间相关关系，提高了海量数据下的分析效率。

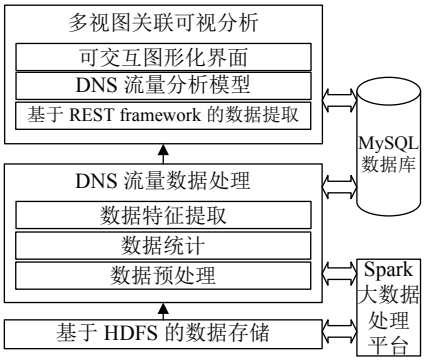

图 2　系统架构

Fig. 2　System architecture

2.2　多视图关联的可视分析

可视分析模块的可交互图形化界面如图3所示，包括数据选择部分和以问题分析为驱动的关联交互视图两部分。

数据选择部分作为分析数据对象的过滤器，所提供的选择包括：DNS基本特征值时序变化趋势分析时间段；DNS请求量和成功解析率时序变化趋势分析时间段；TOP域名分析数量。其中，域名分析数量部分，针对截止2017年4月，半年的DNS流量数据进行了分析，每天请求数为TOP-50的域名访问数约占DNS总请求量的25%，而这50个域名仅占每天请求域名数的0.1%，即：0.1%的域名约占解析总量的1/4，因此将TOP-50的域名进行可视化映射能在一定程度上有效地帮助分析DNS域名解析情况。TOP-20和TOP-100的域名可视映射则分别为解析的TOP域名提供了更详细和更宏观的分析视角。

以问题分析为驱动的关联交互视图建立在TDRI模型之上，包含DNS基本特征值时序变化趋势折线视图；DNS请求量与DNS成功解析率时序变化趋势对比折线视图；特定时间区间内DNS解析域名TOP-*N*柱状视图以及特定域名访问信息平行坐标视图。基于TDRI 4个视图的关联与交互性体现在：1）通过DNS基本特征值时序的变化趋势某时间点关联出当日DNS请求数量和成功解析率的详情对比及当日请求域名TOP-*N*，分别对应图3“关联1”和“关联2”；2）成功解析率的详情对比中，通过DNS请求数趋势某时间点关联出相应分钟内成功解析域名TOP-*N*，通过DNS成功解析率趋势某时间点关联出相应分钟内错误解析域名TOP-*N*，见图3“关联3”。在成功解析率的详情对比坐标系设计缩放的人机交互功能，帮助分析者更细致分析以分钟为时间单位的DNS流量数据；3）通过域名视图中某一特定域名关联出该域名的访问信息，见图3“关联4”。

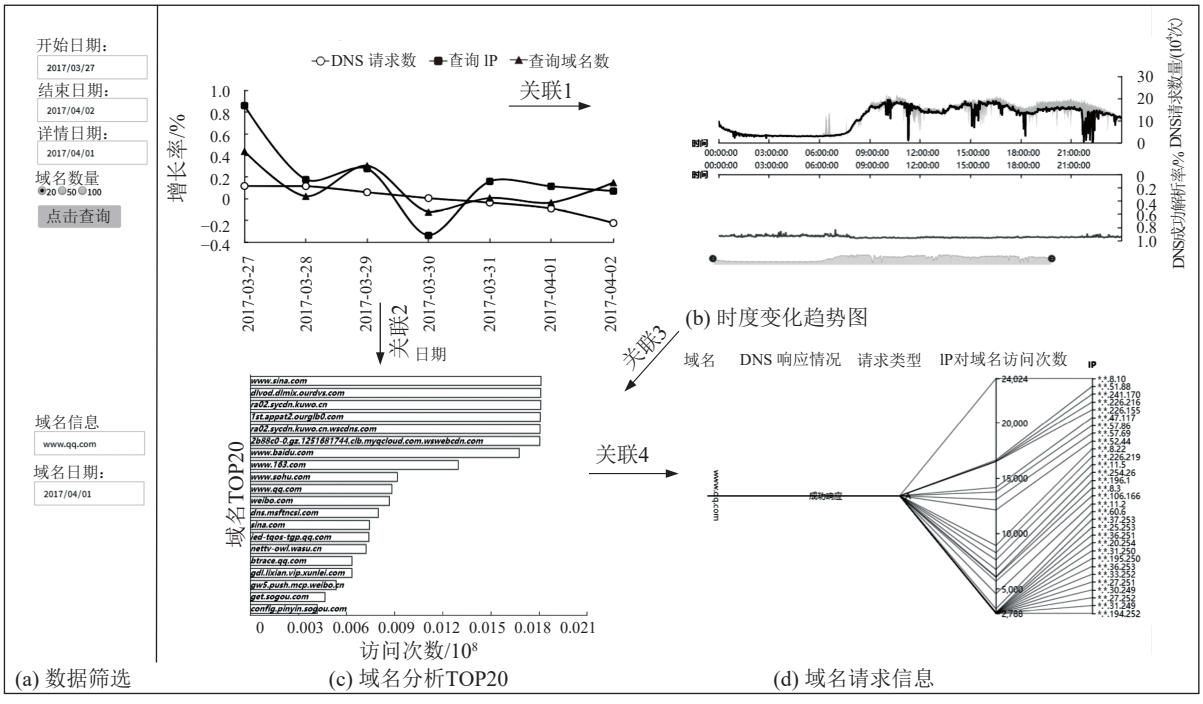

图 3　可交互图形化界面

Fig. 3　Interactive graphical interface

2.2.1　流量特征值变化趋势

DNS请求量、访问者数量和解析域名数量虽存在正相关性，但并未表现出周期性特征。因此在视图处理部分，本文采用增长率描述3个特征的变化程度，以DNS访问量为例，其增长率如下。

$$R=\left(V-\frac{1}{n}\sum_{i=1}^{n}v_i\right)\Big/\left(\frac{1}{n}\sum_{i=1}^{n}v_i\right) \quad (3)$$

式中：V为某天的DNS访问量；n为历史天数；v_i为历史n天中，每天的DNS访问量，本文取$n=3$，$i=1,2,3$。求历史n天均值的做法减小了历史异常值对增长率产生的影响。

将3个特征量增长率按时序对应关系映射到折线图，纵坐标表示选取的3个各特征量的增长率，横坐标表示日期。而以分钟为单位的DNS请求量每天的变化情况随人们的作息时间呈现周期性特征，域名成功解析率则维持在一个相对稳定的值。将单日内DNS请求量和成功解析率按时序进行可视映射，得到分钟粒度下的DNS请求量和解析成功率的对比。并将上述2部分进行图3“关联1”所示视图关联，通过图中左侧某一日期关联出右侧当日请求数量和成功解析率的详情对比。

2.2.2　DNS域名分析

DNS流量特定特征值变化趋势展现特定时间区间内DNS使用情况，分析者通过趋势对比分析定位异常或感兴趣时刻，转入对造成DNS流量特定特征值偏离正常值的域名分析。本文从3个角度筛选DNS解析域名：1）以天为时间单位的解析域名TOP-N；2）以分钟为时间单位的成功解析域名TOP-N；3）以分钟为时间单位的错误域名TOP-N。将DNS流量特征值时序变化趋势视图与域名分析视图关联，包括，通过DNS基本特征值时序变化趋势折线视图中某一日期关联出当日请求域名TOP-N，见图3“关联2”；通过DNS请求量中某一时间点关联出该分钟内成功解析域名TOP-N以及通过DNS成功解析率中某一时间点关联出该分钟内解析失败域名TOP-N，见图3“关联3”。值得一提的是，真实情况下的分析研究发现DNS成功解析率通常相对稳定，分析者对某时刻成功解析率的关注往往由于成功解析率降低。因此本文提出了通过对DNS成功解析率中某一时间点的选择得到解析失败域名TOP-N的关联。

2.2.3　域名访问情况分析

域名分析视图中对域名TOP-N的可视映射帮助分析者定位可疑或感兴趣的域名，进而分析域名访问情况。本文结合域名请求IP、域名请求次数、域名查询类型（type）、DNS返回码（rcode）分析域名访问情况，并通过平行坐标清晰刻画上述5个维度信息间关系。从问题分析驱动的角度，关联域名分析视图与域名访问情况分析视图，见图3“关联4”所示，通过左侧某一特定域名关联出右侧该域名的访问情况。

3　案例分析

为验证上述流量分析模型和可视分析系统的有效性，将上述系统应用到真实环境，以通过交换机镜像得到的作者所在校园内DNS真实流量为数据来源，对2016年11月至2017年4月半年中所采集到的DNS流量进行了分析。

3.1　DNS流量中恶意行为发现与分析

对2017–03–18到2017–03–24一周的数据进行分析时（图4），发现在访问者和DNS解析域名量与历史3 d均值相比持续呈负增长的情况下，DNS总访问量反而出现持续增长，该现象有悖于相关性分析中三者呈正相关的分析结论。相应时间段内DNS成功解析率和DNS访问量对比关系未发现明显异常。进一步的域名分析中，TOP-50域名中出现了一组约15个相似度高且访问量极为相近的域名，结合分钟内访问量并无陡增的情况，推测每分钟上述域名均被大量访问。通过分析每分钟成功解析域名证实了上述推测。接着，查看域名ns4.ourglb0.info的访问情况，出现24个IP对该域名进行了大量成功访问，访问次数集中在76 000次，且这些IP地址本身也存在较大的相似性。对同时段内其余相似域名分析发现其请求者为同一批IP，单日请求量大且相近。该现象从20日持续至23日，结合校园网DNS用户反映DNS使用情况不佳的情况，推测上述IP为消耗网络资源，而对域名进行了恶意持续大量访问。

3.2　疑似DDoS攻击

在对2017年3月23日的DNS流量数据进行分析中，对比DNS访问量和DNS解析成功率趋势发现23日09:04:00分DNS请求数量突增，分钟内DNS请求量从正常状态下约20万次陡增至64万次，该分钟内DNS成功解析率从常态下稳定在90%陡降到27%。判断该分钟内出现针对错误域名的大量请求。通过点击9时4分的DNS解析成功率趋势曲线，得到该分钟内错误请求量TOP-20的域名。这些域名均为对125.69.85网段IP的反向解析域名，且访问量均在约1 900次，如图5所示。由此进一步映射出该分钟内TOP-100的错误解析域名，仍具有上述相似性，可知突然降低的DNS成功解析率由一分钟内被大量请求的反向解析域名导致。结合上述各视图关联分析，该现象疑为一次针对DNS的DDoS攻击。

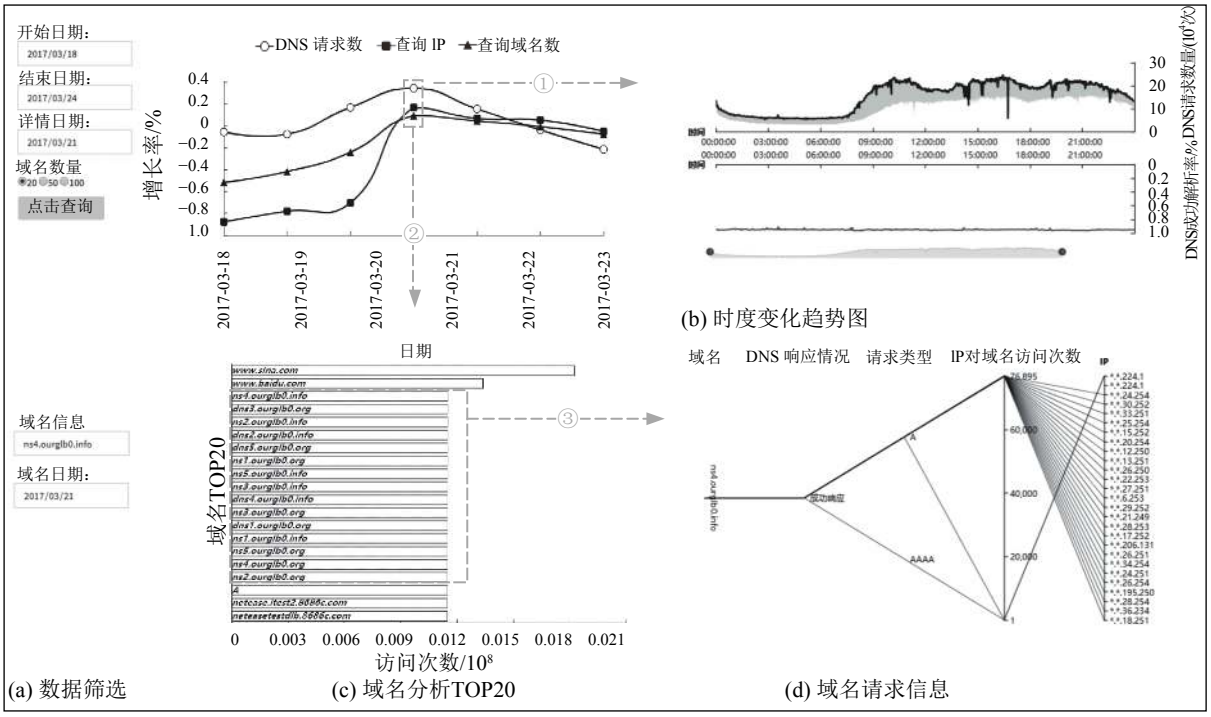

图 4 DNS流量中恶意行为发现与分析

Fig. 4 Discovery and analysis of malicious behavior in DNS traffic

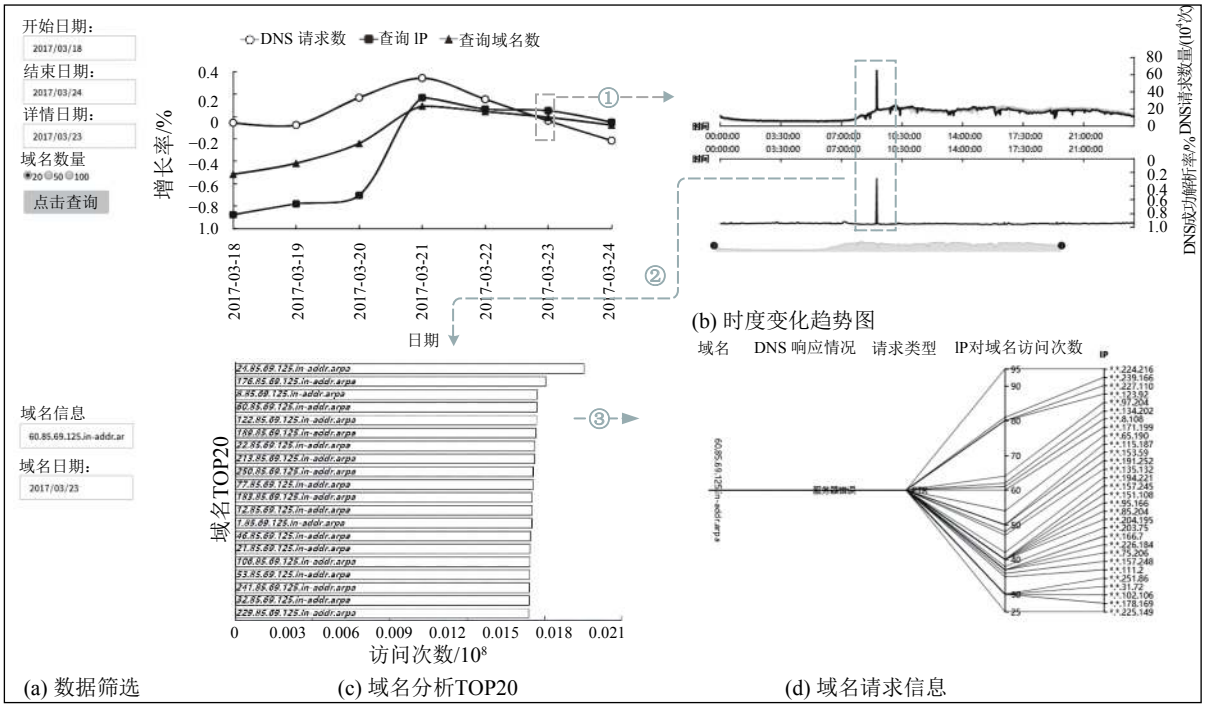

图 5 疑似DDoS攻击发现与分析

Fig. 5 Suspected DDoS attack discovery and analysis

4 结 论

通过对DNS实际流量的观测分析，提出了基于TDRI的DNS流量分析模型，该模型包含流量特征属性值时序化趋势分析、请求域名分析及域名访问情况分析3个层面的分析过程。在此基础上设计了以问题分析为驱动的多视图关联DNS流量可视分析系统，实现了基于TDRI的多视图关联DNS流量可视分析。该系统应用于实际环境后，支撑了海量DNS数据的高效分析，有效检测DNS流量中表现出的恶意行

为，发现了校园网DNS面临的安全问题。在下一步研究中，本文将继续完善DNS流量分析模型，关注更多DNS特征之间的关联性，并优化可视分析方式。

参考文献：

[1] Li Jie.The detection of DNS spoofing and cache poisoning attack[D].Chengdu:University of Electronic Science and Technology,2015.[李杰.DNS欺骗和缓存中毒攻击的检测[D].成都:电子科技大学,2015.]

[2] Chen Lin.Research on DNS attack detection and defense technology[D].Beijing:Beijing University of Posts and Telecommunications,2011.[陈琳.DNS攻击检测与防御技术研究[D].北京:北京邮电大学,2011.]

[3] Zhang Siyu.Detecting malware domains on DNS traffic [D].Shanghai:Shanghai Jiao Tong University,2014.[章思宇.基于DNS流量的恶意软件域名挖掘[D].上海:上海交通大学,2014.]

[4] Zhang Weiwei,Gong Jian,Liu Shangdong,et al.DNS surveillance on backbone[J].Journal of Software,2017,28(9):2370–2387.[张维维,龚俭,刘尚东,等.面向主干网的DNS流量监测研究[J].软件学报,2017,28(9):2370–2387.]

[5] Miao Chen.The analysis and study on internet DNS traffic [D].Beijing:Beijing University of Posts and Telecommunications,2012.[缪晨.互联网DNS流量分析与研究[D].北京:北京邮电大学,2012.]

[6] Lü Liangfu,Zhang Jiawan,Sun Jizhou,et al.Survey of network security visualization techniques[J].Journal of Computer Applications,2008,28(8):1924–1927.[吕良福,张加万,孙济洲,等.网络安全可视化研究综述[J].计算机应用,2008,28(8):1924–1927.]

[7] Shiravi A,Shiravi H,Ghorbani A A.A survey of visualization systems for network security[J].IEEE Transactions on Visualization & Computer Graphics,2012,18(99):1313–1329.

[8] Zhao Ying,Fan Xiaoping,Zhou Fangfang,et al.A survey on network security data visualization[J].Journal of Computer-Aided Design and Computer Graphics,2014,26(5):687–697.[赵颖,樊晓平,周芳芳,等.网络安全数据可视化综述[J].计算机辅助设计与图形学学报,2014,26(5):687–697.]

[9] Chen Xingshu,Zeng Xuemei,Wang Wenxian,et al.Big data analytics for network security and intelligence[J].Advanced Engineering Sciences,2017,49(3):1–12.[陈兴蜀,曾雪梅,王文贤,等.基于大数据的网络安全与情报分析[J].工程科学与技术,2017,49(3):1–12.]

[10] Hao L,Healey C G,Hutchinson S E.Flexible web visualization for alert-based network security analytics[C]//Proceedings of the Tenth Workshop on Visualization for Cyber Security.Atlanta GA:ACM,2013:33–40.

[11] Chen S,Guo C,Yuan X,et al.Oceans:Online collaborative explorative analysis on network security[C]//Proceedings of the Eleventh Workshop on Visualization for Cyber Security.Paris:ACM,2014:1–8.

[12] Zhao Ying,Wang Quan,Huang Yezi,et al.Collaborative visual analytics for network traffic time-series data with multiple views[J].Journal of Software,2016,27(5):1188–1198.[赵颖,王权,黄叶子,等.多视图合作的网络流量时序数据可视分析[J].软件学报,2016,27(5):1188–1198.]

[13] Yan Fen,Ding Chao,Yin Xinchun.Research on exploiting dos attack against DNS based on information entropy[J].Computer Science,2015,42(3):140–143.[严芬,丁超,殷新春.基于信息熵的DNS拒绝服务攻击的检测研究[J].计算机科学,2015,42(3):140–143.]

[14] Liang Jiye,Feng Chenjiao,Song Peng.A survey on correlation analysis of big data[J].Chinese Journal of Computers,2016,39(1):1–18.[梁吉业,冯晨娇,宋鹏.大数据相关分析综述[J].计算机学报,2016,39(1):1–18.]

[15] Ren Lei,Du Yi,Ma Shuai,et al.Visual analytics towards big data[J].Journal of Software,2014,25(9):1909–1936.[任磊,杜一,马帅,等.大数据可视分析综述[J].软件学报,2014,25(9):1909–1936.]

（编辑　张凌之）

引用格式：Chen Xingshu,Chen Jinghan,Zeng Xuemei,et al.Correlative visual analytics for DNS traffic with multiple views based on TDRI[J].Advanced Engineering Sciences,2018,50(4):123–129.[陈兴蜀,陈敬涵,曾雪梅,等.基于TDRI的多视图关联DNS流量可视分析[J].工程科学与技术,2018,50(4):123–129.]