政府教育域名权威资源记录异常变更测量研究

孙俊哲，陆超逸，刘保君，段海新，孙东红
（清华大学网络科学与网络空间研究院，北京 100084）

摘　要：权威侧域名劫持伴随资源记录异常变更。为实现权威侧域名劫持事件的及时预警，针对各国政府、教育等重要行业域名和高访问量的流行域名，构建权威侧资源记录监测系统，实现对全球750万个重要域名的主动抓取和长期监测。提出资源记录异常变更筛选算法并应用于监测数据，在一个月的分析周期内识别896个重要域名的资源记录存在异常变更。经人工验证，导致资源记录异常变更的原因包括域名管理者的不当配置、钓鱼攻击和非法内容展示等行为。

关键词：域名系统；资源记录；权威服务；劫持攻击
中图分类号：TN915.08
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024252

Measurement study on abnormal changes in authoritative resource records of government and educational domains

SUN Junzhe, LU Chaoyi, LIU Baojun, DUAN Haixin, SUN Donghong
Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China

Abstract: Authoritative-side domain hijacking is characterized by abnormal changes in resource records. To enable timely warnings for authoritative-side domain hijacking incidents, a monitoring system for authoritative-side resource records was established, targeting significant domains in key sectors such as government and education, as well as high-traffic popular domains. The system actively captured and continuously monitored 7.5 million important domains globally. An algorithm was developed to filter abnormal changes in resource records, identifying abnormal changes in 896 significant domains within a one-month analysis period. Manual verification results indicate that the causes included misconfigurations by domain administrators, phishing attacks, and the display of illegal content.

Keywords: domain name system, resource records, authoritative service, hijacking attack

0　引言

域名系统（DNS, domain name system）是互联网的关键基础设施之一，负责将方便用户记忆的域名映射至计算机能够处理的IP地址。DNS不仅支撑了诸如网页浏览、电子邮件等大量互联网上层应用的稳定运行，也为数字证书签发等网络安全服务提供信任基础。DNS在互联网中的关键作用，使它成为网络攻击者重点关注的目标，域名系统劫持（DNS Hijacking）便是其中一种影响严重的攻击形式：攻击者通过篡改域名解析过程和报文内容，将用户的网络请求引导至恶意网站，进而造成网络钓鱼、恶意代码分发等后果。例如，2010年百度域名遭到劫持[1]，导致搜索引擎主页被恶意涂改长达8小时，造成超过700万元的直接经济损失。

就攻击技术而言，已有较多的研究揭示了多种针对域名解析过程的劫持，包括客户端DNS配置篡改[2]、中间人报文劫持篡改[3-4]、域名解析路径劫持[5]，以及搭建恶意或虚假的域名服务器镜像[6-7]等。上述安全威胁的根源在于DNS缺乏消息完整性保障和身份认证机制，导致接收方无法验证

收稿日期：2024–08–21

消息来源和正确性。随着域名系统安全扩展（DNSSEC）[8]、DNS cookie[9]、加密 DNS 协议[10]等安全技术的提出和部署推广，上述风险均能得到不同程度的缓解。

然而，近年来网络安全机构披露了一种新型的隐蔽域名劫持手段，即权威侧的资源记录异常变更。不同于传统劫持域名解析报文的方法，攻击者通过窃取域名管理账号、利用注册商管理漏洞等方式直接获取目标域名的控制权，进而篡改其权威资源记录指向恶意站点。已披露的劫持事件多选择政府、教育等重要行业域名作为攻击目标，产生严重的安全威胁[11-12]。为逃避打击，攻击者通常间歇性、短时且隐蔽地进行资源记录的恶意篡改[13]，待每轮攻击完成后即将域名恢复原状，因此现有的域名劫持检测方法和历史资源记录数据集不足以准确观测此类行为。

为实现权威侧记录异常变更现象的大规模监测并提供及时预警，本文设计实现了权威侧资源记录大规模监测系统 DomainWatch，针对全球各国政府、教育等重要行业域名和高访问度的流行域名开展监测。系统包含域名收集、数据抓取和数据存储 3 个模块，向目标域名的权威服务器发起主动查询，对其提供的资源记录进行长时间、高频次的监控，构建可检索的大规模域名资源记录历史数据库。2024 年 1 月至 7 月期间，系统已实现对全球 750 万重要域名以 4 小时为周期的监测，收集并索引的资源记录条目数量达到 7.4 亿。

在具备重要域名高频历史资源记录数据的基础上，本文提出多维信息关联的资源记录异常变更筛选算法 HijackHound。针对权威侧劫持行为的隐蔽短时特点，算法引入时间窗口并综合 IP 归属地、HTTP 页面内容、数字证书等多维域名特征，筛选可疑的变更现象。在一个月的分析周期内，超过 90% 的被监测域名未出现资源记录的任何变化。算法共预警 896 个域名存在资源记录的异常变更现象，涉及多国政府、高校、媒体等重要机构以及高访问量域名。大部分异常变更持续时间不超过 4 小时即被恢复原状，少量域名的权威服务器一并发生短暂的变更，且部分修改后的临时 IP 地址与黑名单重合，显示出潜在的恶意行为动机。经进一步的人工验证，资源记录异常变更的原因包括域名管理不当导致的错误配置、钓鱼攻击，以及非法内容展示等行为。

本文研究表明，重要域名的权威资源记录异常变更现象时有发生且存在较大安全风险，通过资源记录主动收集和筛选能够有效实现及时预警。因此，建议各方提高对这一现象的认知，加强对重要域名管理权限和账号的管理，同时通过定期自查减少域名的错误配置。此外，对于重要域名应当建立权威侧资源记录长期监测机制；本文提出的系统将持续运行，帮助域名管理者排查配置错误，为监管部门及时发现权威侧域名劫持现象提供依据，对可疑的攻击行为进行及时预警和处置。

1　技术背景与相关工作

1.1　域名解析过程与权威侧域名劫持

互联网域名解析是通过查询将域名转换为与之对应的 IP 地址或其他互联网资源的过程。互联网域名解析过程如图 1 所示，客户端设备向递归解析器发送域名解析请求，后者将依次查询根服务器、顶级域名和二级域名的权威服务器，得到解析结果并返回客户端。各级权威服务器由域名所有者自行配置，存储着域名的解析结果；当收到下级域名的

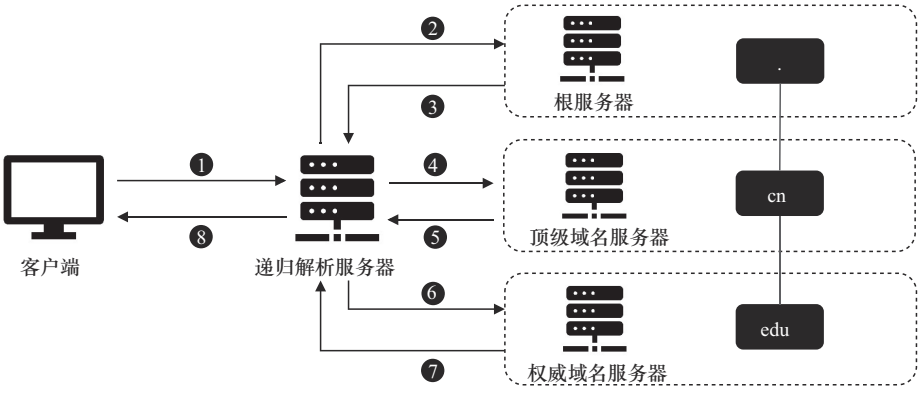


图 1　互联网域名解析过程

查询时，权威服务器还将返回下一级域名的权威服务器名称，使这一解析过程能够继续进行。

权威侧资源记录变更，指权威服务器存储的资源记录发生改变。这种变更可能是由域名所有者发起的正常行为，例如域名配置升级或所有权发生迁移，导致域名指向的IP地址发生变化。研究表明，此类正常的变更现象通常是持续性的[13]，例如，指向IP地址变化后即长时间维持，不再回退至原地址或短时间内再次发生变化。而相对应地，资源记录在短期内发生非预期的临时变化则较为可疑，称为异常变更。权威侧域名劫持过程如图2所示，通过窃取域名管理账号、利用域名注册商管理漏洞等方式直接获取目标域名的控制权，进而篡改域名资源记录指向含有恶意内容的IP地址，劫持用户的访问流量。

在获取域名权威侧的控制权后，为提高后续恶意行为的隐蔽性，根据已曝光的劫持事件分析，此类资源记录异常变更现象具有如下特征。首先，资源记录通常是临时发生变化，被篡改的新记录存续时间较短（通常不超过一天），随后即回退至原有的正常配置。例如，2014年法国航天企业Safran Aircraft Engines的资源记录遭到恶意篡改[12]，被修改的资源记录在仅几分钟后即被攻击者恢复原状。这样的策略不仅可以防止劫持行为出现在每日全网的区域文件快照和主动监测数据中，而且可以避免由于流量长时间减少而触发域名管理者设置的安全警报。同时，攻击者大量使用公共云服务器地址搭建恶意网站，因此与域名的原始IP地址通常位于不同的网络和地理位置。此外，为了获取用户和浏览器的信任，多数攻击者同时选择在恶意网站上配置目标域名的数字证书；然而，由于原始数字证书无法被伪造，攻击者只能为目标域名申请新证书，而新旧证书将在日期、公钥等字段存在不同。

1.2　国内外研究现状

对于各类域名劫持现象，已有研究工作大多关注针对域名解析过程的劫持。在客户端侧，Dagon等[2]发现一些恶意的URL在被访问时将篡改客户端的DNS配置指向恶意的解析服务，进而实现流量劫持。在递归域名服务器侧，Kührer等[6]发现部分互联网上的公共递归域名服务器刻意对特定域名返回错误的解析结果。在链路层面，Weaver等[3]发现部分运营商篡改DNS应答报文，指向包含广告的页面并以此谋取利润；Liu等[5]发现部分中间设备伪造成知名的DNS服务响应用户的域名查询，劫持域名的解析路径。

由于具有强隐蔽性和短时性等特点，针对权威侧域名劫持和资源记录异常变更的监测工作则较为困难和少见。Houser等[14]使用机器学习的方法训练检测模型，然而过度依赖已知的劫持事件，难以保证检测未知事件的准确性。Akiwate等[13]利用现有数据集和启发式规则识别出少量攻击者使用的基础设施，但由于数据集的更新频率低，只能识别出因攻击者操作失误而出现长期劫持的域名。

针对政府、教育等重要行业域名建立权威资源记录的主动监测系统，有助于实现异常变更现象的及时预警；然而，现有的域名资源记录历史数据库

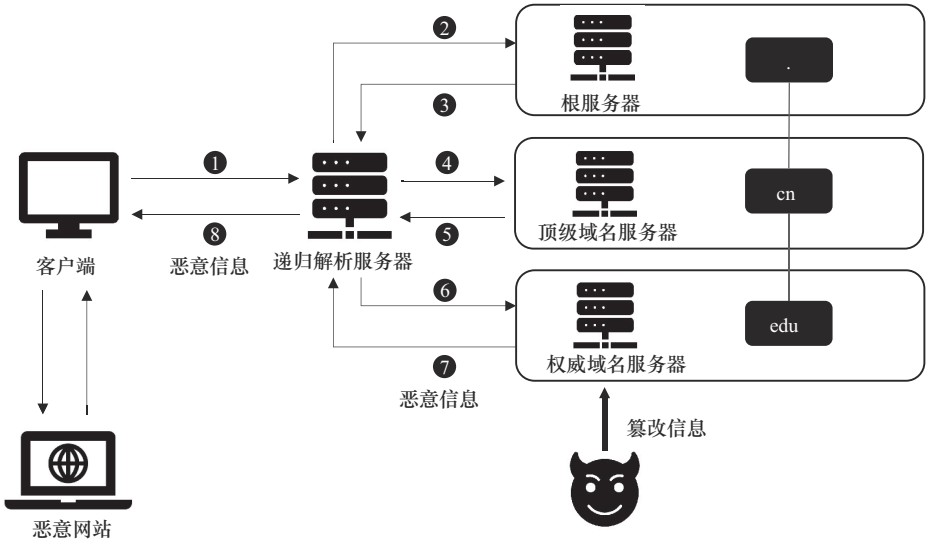


图2　权威侧域名劫持过程

无法满足这一需求。OpenINTEL[15]针对多个通用顶级区域和国家顶级区域中总计2.18亿个二级域名，以天为单位主动爬取它们的资源记录；Thales[16]主要针对公共黑名单或威胁情报中的域名，以天为单位主动爬取；Rapid 7[17]主要的监测目标是在数字证书和HTTP爬虫中所见的域名，监测频率为一周一次。这些系统的监测频率均较低，难以发现并记录具有短时性和隐蔽性的权威侧异常变更现象；此外，政府、教育等行业域名具有显著的重要性，且是权威侧域名劫持的主要受害者。然而，现有数据集均未将它们纳入监测范围。

2　域名权威侧资源记录监测系统构建

2.1　系统设计需求

系统的设计目标是针对政府、教育等重要行业以及高访问量的流行域名，开展权威资源记录的长时间、高频次监控，形成可检索的资源记录历史数据库，支撑异常变更现象和劫持行为的筛选和分析。系统设计应具备规模性，即监测范围覆盖全球各国重要域名的主要资源记录类型；采集高实时性，即实现大量域名实时资源记录的快速、高频次主动抓取，捕捉短时内发生的资源记录变化；数据高可用性，即有效控制高频监测过程中出现的重复和冗余，并支持进行任意条件（如给定时间窗口）下的高效检索利用。

基于上述设计需求，系统分为域名收集模块、数据抓取模块和数据存储模块，分别实现规模性、采集高实时性和数据高可用性目标。重要域名权威侧资源记录监测系统DomainWatch工作流程如图3所示。

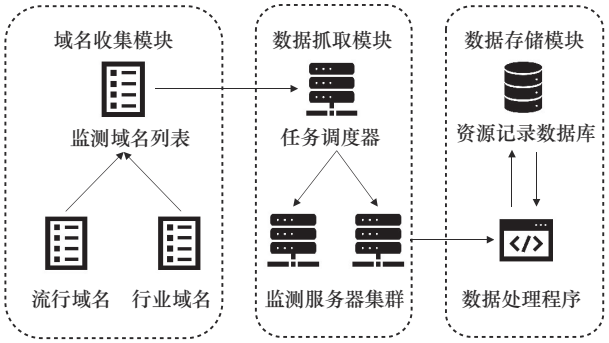


图3　重要域名权威侧资源记录监测系统DomainWatch工作流程

2.2　域名收集模块

系统监测的重要行业域名主要涵盖全球各国的政府网站和教育网站。然而，由于这2个行业的域名具有特殊的重要性，相关的注册管理机构通常不会对外公开区域文件，因此无法直接获取公开完整的域名列表，需要采用特殊的方式构造。

一般情况下，政府和教育网站域名的主要特征是，其后缀由特定字符串（gov或edu）和国家顶级域名（如cn）组成。然而，实际上还存在一些其他的后缀与这2个行业相关，如gob和gouv分别在西班牙语和法语中与gov同义，教育机构也同时包括与学术机构相关的.ac和与学校相关的.sch等后缀。因此，通过搜索引擎和人工筛选结果，最终枚举17个与政府机构相关和12个与教育机构相关的后缀，如表1所示。将它们与国家顶级域名拼接形成域名后缀，并仅保留出现在公共后缀列表（PSL, public suffix list）中的后缀。

表1　政府教育行业域名后缀集合

行业类别	域名后缀（省去国家顶级域后）
政府网站	gov, admin, bel, canada, gc, gob, gok, gkp, go, gog, gop, gos, gouv, govt, gub, gv, lg
教育网站	edu, ac, ed, es, hs, k12, kg, ms, sc, sch, school, univ

在确定域名后缀范围后，为列举政府教育行业相关的二级域名，利用国内某安全公司维护的大型Passive DNS数据，从中查找使用上述后缀的所有历史活跃域名。Passive DNS是一种域名解析日志，从中可以获取活跃域名在某段时间内的解析结果。最终，共收集到共50万个政府、教育行业二级域名，覆盖135个国家，将其全部纳入监测范围。

在高访问的流行域名方面，选取Tranco域名流行度排名列表[18]中的前100万个域名。Tranco是一个全球性的网站排名数据集，收集并整理了数百万个网站的排名信息。为了保证监测域名的实时性和全面性，系统每月更新一次流行域名列表。

对于所有纳入监测范围的域名，除二级域名本身之外，额外补充了对其重要子域名（含www、mail、login、admin）的监测。上述子域名提供了关键的网站基础服务，易成为劫持攻击目标。最终，域名收集模块共输出750万需纳入监测范围的域名，包含135个国家的政府教育行业、高访问流行域名及其子域名，实现了监测范围的规模性。

2.3　数据抓取模块

对于列表中的每一个域名，数据抓取模块查询其权威服务器地址，并定期访问所有权威服务器以

分别收集权威侧资源记录。针对异常变更现象的短时特点，将监测周期设置为4小时，收集的资源记录类型包括A（IPv4地址）、AAAA（IPv6地址）、NS（权威服务器名称）、CNAME（别名）、SOA（起始授权）和MX（邮件服务器）。

数据抓取模块由多台服务器构成，分别充当任务调度器和数据收集器，并行完成给定任务。任务调度器将整体的域名列表拆分为多个子列表，将拆分后的任务分发下达至各个数据收集器并行执行。为实现大量域名的高实时抓取，系统的数据收集器使用独立的裸金属（bare metal）服务器，可以直接生成以太网帧，绕过网络堆栈中的中间层并以接近线性的速度进行扫描，满足高频收集大规模域名资源记录的需求。

实时查询权威服务器获取资源记录的功能，使用开源工具ZDNS[19]实现。ZDNS使用Go语言编写，可以管理数千个轻量级例程实现高效并发，并且在重用UDP端口等性能方面做了一系列优化，能够实现大规模资源记录的快速获取。此外，ZDNS支持自行迭代查询和遍历域名服务器查询，可以不借助第三方的递归解析器，自行实现递归解析器的功能，收集每一个权威服务器处的资源记录数据，排除中间链路和第三方递归解析器对资源记录结果的干扰，保证资源记录来源于权威侧。ZDNS输出的原始资源记录将以JSON格式表示。

2.4 数据存储模块

系统以小时为周期收集多达750万域名的若干种资源记录，在变更频率普遍不高的情况下，数据量庞大且存在大量重复和冗余。为实现数据的高可用性、提高存储和分析效率，需要设计高效的存储数据结构，对原始数据进行清洗和合并。

数据存储模块首先去除查询超时和失败的内容，只保留查询状态为正确（NOERROR）的结果。对于每个原始文件中存储的信息，提取出查询域名QNAME、数据来源服务器名称Server、响应结果字段RDATA和生存时间TTL。同时，参照Passive DNS数据库的格式设计，引入首次观测和末次观测时间戳，直接合并连续时间跨度内出现的多条完全相同的数据条目，去除冗余并大幅节省存储空间。为实现数据库的快速检索、进一步减小存储空间需求，经合并后的数据将由JSON格式转为Apache Avro格式，并最终转为Parquet列式存储格式。列式存储格式只需要读取单独的QNAME列，而并不需要遍历整个数据集，可以最小化I/O过程，大幅提高查询效率。

经过上述数据处理流程，系统形成的每月数据所需存储空间由300 GB降低至1 GB。将每日更新的Parquet文件分别存储入MySQL数据库并建表，具体字段如表2所示。经入库的域名历史资源记录可以通过SQL语句的方式查询。图4展示了系统获取到的cernet.edu.cn域名的历史权威侧资源记录（A类型）、各条记录的来源服务器以及存续时间。

表2 域名历史资源记录字段

字段名称	类型	字段描述
domain	文本	被监测域名
nameserver	文本	数据来源（权威服务器）
rdata	文本	资源数据
ttl	整数	资源记录生存时间
first_seen	文本	首次观测时间
last_seen	文本	末次观测时间
count	整数	资源记录被观测到的次数

2.5 运行效率评估

系统设定单次DNS查询超时时间为5 s，单个域名解析流程的总超时时间为15 s，降低因偶然超时发生的收集错误，同时保证所有域名的数据收集过程在4小时周期内执行完毕。通过Crontab定时程序实现自动运行，每日共产生70 GB的上行流量和120 GB的下行流量。每月构建域名列表需要10 s，

```
[sunjunzhe@localhost active_dns_scan]$ python search.py --rtype a --domain cernet.edu.cn
```

Domain	Nameserver	Rdata	TTL	First_seen	Last_seen	Counts
cernet.edu.cn	dns.edu.cn	202.205.109.203	86400	2024-01-01-00	2024-08-08-21	1902
cernet.edu.cn	dns2.edu.cn	202.205.109.203	86400	2024-01-01-00	2024-08-08-21	1901
cernet.edu.cn	ns2.cuhk.edu.hk	202.205.109.203	86400	2024-01-01-04	2024-08-08-20	783

图4 cernet.edu.cn的历史权威侧资源记录

每次收集完成750万域名的共6项资源记录需要3小时，每日完成所有域名的数据处理和存储需要1小时，查询任意域名的数据可以控制在0.1 s内。经过效率评估和实际运行测试，系统满足对重要域名资源记录的长时间、高频次监测目标。

3　资源记录异常变更现象筛选

3.1　筛选算法设计

算法的设计目标是结合域名的历史资源记录数据，通过IP归属地、HTTP页面、数字证书等多维度信息的筛选，有效、及时分析出异常变更现象和原因。因此，算法的流程分为短暂变更现象检测、异常变更现象筛选和异常原因分析，如图5所示。

资源记录临时变更识别。如前文描述，权威侧劫持攻击单次持续通常不超过一天即恢复原状，正常的变更则会长时间维持；因此，异常的资源记录变化只在某个短期区间内发生，而在更长的时间跨度内不应存在显著差异。根据这一基础观察，本文选取短期窗口w_1（1天）和长期窗口w_2（3天），集合S_1~S_4是检测日期t前后短期和长期窗口内出现的资源记录集合，如图6所示。

通过分别评估S_1与S_2的JACCARD距离及S_3与S_4的JACCARD距离，差值score为正值的域名意味着在该日期发生了资源记录的临时变更，score为非正值的域名意味着在检测日期发生了资源记录的正常变更（如域名配置了负载均衡技术或管理者正常更改IP地址等操作），计算式如下

$$S_1 = \{ \mathrm{RR}_{\mathrm{rdata}} | \mathrm{RR}_{\mathrm{first}} \leqslant t, \mathrm{RR}_{\mathrm{last}} \geqslant t - \frac{w_1}{2} \}$$

$$S_2 = \{ \mathrm{RR}_{\mathrm{rdata}} | \mathrm{RR}_{\mathrm{first}} \leqslant t + \frac{w_1}{2}, \mathrm{RR}_{\mathrm{last}} \geqslant t \}$$

$$S_3 = \{ \mathrm{RR}_{\mathrm{rdata}} | \mathrm{RR}_{\mathrm{first}} \leqslant t - \frac{w_1}{2}, \mathrm{RR}_{\mathrm{last}} \geqslant t - \frac{w_2}{2} \}$$

$$S_4 = \{ \mathrm{RR}_{\mathrm{rdata}} | \mathrm{RR}_{\mathrm{first}} \leqslant t + \frac{w_2}{2}, \mathrm{RR}_{\mathrm{last}} \geqslant t + \frac{w_1}{2} \}$$

$$\mathrm{JD}(A,B) = 1 - \left| \frac{A \cap B}{A \cup B} \right|$$

$$\mathrm{score} = \mathrm{JD}(S_1,S_2) - \mathrm{JD}(S_3,S_4) > 0$$

多维域名特征判断。在检测形成临时变更列表后，由于攻击者控制的IP地址通常与域名管理者的IP地址位于不同的地理位置和网络位置，检查临时存在的IP地址所属互联网自治系统（AS, autonomous system）和国家，只保留临时IP地址与原始IP地址属于不同自治系统或国家的域名。此外，为减少误报，排除在Passive DNS数据集中临时IP地址长期为该域名或相关子域名历史解析结果的情况；这种情况通常是域名所有者的正常配置所导致（如出于技术原因，临时启用曾弃用的服务

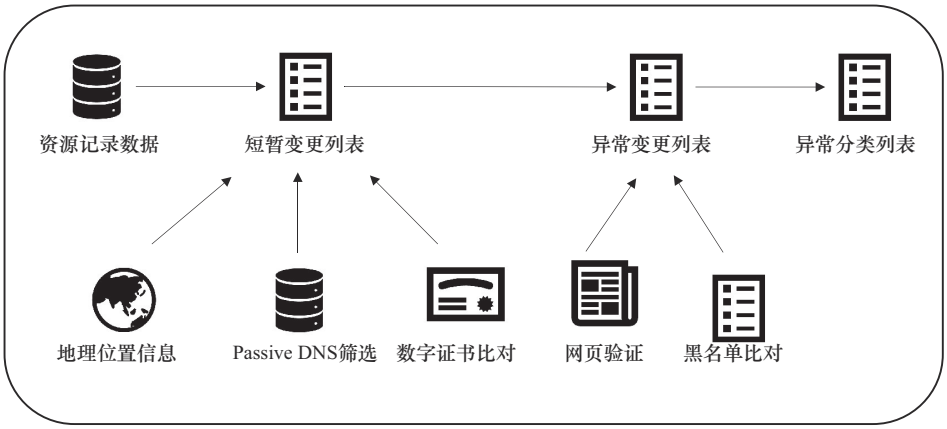


图5　资源记录异常变更筛选算法流程

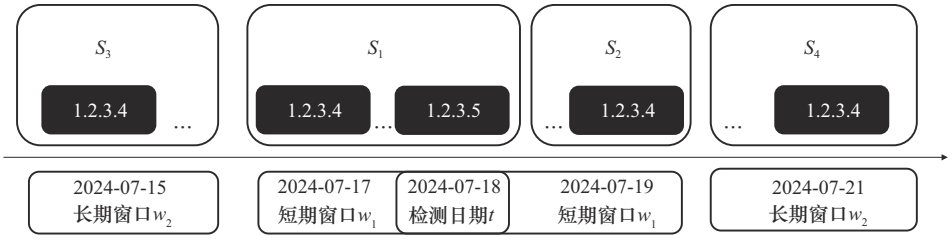


图6　资源记录临时变更识别示意图

器地址），故不考虑其为异常变更现象。最后，攻击者为通过用户浏览器的安全检测，需要持有相关域名的证书，而该证书与域名管理者拥有的证书不同。算法重点筛选临时IP地址和原始IP地址上部署的证书不一致的域名，该行为不符合正常的域名管理措施，属于异常现象。

资源记录异常变更现象的原因分析。根据形成的异常变更列表，为了进一步确认异常原因，获取了临时IP地址和原始IP地址上部署的域名页面进行人工比对，并结合IP黑名单[20]、DNS黑名单[20]和DNS劫持域名名单[21]，对检测出的异常域名进行分类，总结出异常变更的原因，并给出相应的异常分类列表。

3.2　异常变更规模

选取2024年7月1日至7月31日系统获取的资源记录数据作为分析周期，识别在此期间重要域名资源记录发生的异常变更现象。在一个月的周期内，超过90%的被监测域名未发生任何类型资源记录的任何变化（短期或长期），表明重要域名的资源记录配置通常相对稳定，进一步说明资源记录的临时变更现象本身即存在疑点。应用临时变更筛选条件后，判定有18 242个域名的权威侧IP地址发生过临时变更，且临时IP地址与原始IP地址位于不同的地理位置和网络位置。其中，84.7%的域名资源记录变更持续时间不超过4小时，符合异常变更现象的基本特点。进一步应用数字证书筛选条件后，临时IP地址上的数字证书与原证书不一致的域名有896个，构成存在异常变更现象的域名列表。

存在资源记录异常变更的域名中，发现21.7%域名在指向临时IP地址的同时，其NS类型资源记录同时被修改，将配置权临时转入了外部的域名托管平台。表3列举了存在异常变更的域名中，转入数量排名前5的域名托管服务商及相关的域名数量。

表3　转入数量排名前5的域名托管服务商及相关的域名数量

域名托管服务商	转入域名数量	占比
Cloudflare	55	6.1%
GoDaddy	45	5.0%
Foundationapi（域名停放服务）	19	2.1%
eNom	13	1.5%
NameSilo	8	0.9%

在异常变更域名列表中，各国政府和教育行业相关域名分别占比2.3%和8.1%。表4列举了不同行业存在异常变更现象的域名数量排名前5的国家。值得注意的是，在2024年7月这一分析周期内，我国的政府（gov.cn）和教育（edu.cn）行业域名未发现存在资源记录的临时异常变更现象。

表4　不同行业存在异常变更现象的域名数量排名前5的国家

国家	政府域名数量	国家	教育域名数量
印度尼西亚	6	印度尼西亚	34
阿根廷	3	越南	8
美国	3	波兰	8
英国	2	巴基斯坦	6
秘鲁	2	印度	4

本文对资源记录异常变更的原因进行了分析。通过人工比对页面和黑名单等方式，将原因总结至表5。其中，最常见的异常变更由域名管理者的操作失误或临时措施引起，占比89.6%。然而，从部分域名的HTTP页面发现了疑似钓鱼攻击和恶意行为，也发现了部分变更后的临时IP地址命中黑名单。

表5　异常变更原因

异常原因		域名数量	占比
域名管理不当	域名错误配置	482	53.8%
	域名临时停放	129	14.4%
临时管理措施	服务临时转移	183	20.4%
	网站临时维护	9	1.0%
疑似攻击行为	钓鱼攻击	1	0.1%
	非法内容展示	2	0.2%
	DNS黑名单	41	4.6%
	IP黑名单	47	5.2%
	DNS劫持名单	2	0.2%

在疑似攻击行为中，临时的数字证书是判定攻击行为的关键因素。表6统计了排名前5的临时证书签发机构。可以看出，知名且稳定的证书签发机构GoDaddy和免费且自动化的证书签发机构Let’s Encrypt在变更后的临时IP地址上应用广泛。

表 6　签发临时证书数量排名前 5 的证书签发机构

证书签发机构	签发域名数量	占比
GoDaddy	41	44.1%
Let’s Encrypt	27	29.0%
Google Trust Services	10	10.8%
Amazon	4	4.3%
DigiCert	2	2.2%

3.3　典型案例分析

域名管理不当导致的错误配置。域名错误配置是最常见的权威资源记录异常变更原因。由于域名管理者的操作不当，将域名指向了无效或异常的 IP 地址，导致无法正常访问。大多数错误配置的结果是无法获取任何页面。例如，巴西教育机构 FPC（教育行业）的网站在 2024 年 7 月 8 日 16 时发生资源记录异常变更，从临时服务器上无法获取到 HTTP 页面，致使该网站的服务临时中断。另一种情况是域名管理者意外地配置了曾经使用过的、已被淘汰的历史页面。例如，印度的 Pmchri 医学院（教育行业）网站在 7 月 3 日 0 时发生资源记录变更，临时页面是一个 Web 服务器目录，文件夹名称显示与该域名相关，但修改时间均为 2022 年，可能是域名管理者错误地配置了该机构曾使用过的旧版域名和网页。在少数情况中，域名管理者错误地上线了用于调试的网页。例如，波兰的 Cudmoda 购物网站（高访问量，Tranco 流行度排名约 48 万位）在 7 月 10 日 12 时变更至临时 IP 地址，其页面末尾存在大量 JavaScript 代码和页面加载时间、内存使用、调用后台 SQL 语句（含表名、变量名等，如图 7 所示）等调试信息，降低页面加载速度的同时，导致站点后台信息泄露风险。

域名临时停放。域名临时停放是另一种常见的异常变更原因，指域名到期后由注册机构临时指向停放页面，待续费后恢复正常服务。与域名停放服务商相关的权威服务器列表和 IP 地址列表[22]相比对，筛选因停放导致的异常变更，发现异常变更列表中域名临时停放至的服务商主要为 BODIS 和 Sedo。例如，IT 技术支持公司 DailyComputers（高访问量，Tranco 流行度排名约 37 万位）的网站在 2024 年 7 月 3 日 8 时发生资源记录异常变更，IP 地址临时变更至域名停放服务商 Sedo 的网段。根据域名的 WHOIS 信息，该域名是 1999 年 7 月 1 日注册的，因此每年的 7 月初应当及时续费。目前该域名的 WHOIS 信息显示，其信息的最近更新时间为 2024 年 7 月 3 日，域名过期时间为 2025 年 7 月 1 日，符合对于域名因为过期而停放的判断。

网站服务节点临时转移。当网站的主服务器遇到特殊情况时，域名管理者可能会将网站服务临时切换到备用服务器。特殊情况包括硬件升级、软件更新、故障恢复等维护工作，也包括在流量高峰期临时启用的负载均衡策略。例如，越南的 Cdythadong 医学院（教育行业）网站在 2024 年 7 月 2 日 4 时发生了资源记录的异常变更，而访问后的网页页面本身没有任何变动。这种情况可以认为是网站的主服务器临时遇到了特殊情况，在很短的时间内即得到了及时的纠正，对用户的影响较小。

网站临时下线维护。在网站整体存在故障需要维护时，域名管理者可以将域名临时部署到备用的服务器上，并配置专门的网页来告知用户。例如，澳大利亚南澳职业技术学院 TAFE SA 和越南的 TDMU 大学（教育行业）分别于 2024 年 7 月 2 日 16 时和 7 月 10 日 4 时进行了临时的网站维护，并在临时服务器上部署了通知页面，如图 8 所示。

钓鱼攻击。钓鱼攻击是指攻击者伪造与原网站相似的页面，诱导用户输入账号和密码等敏感信息，侵犯用户利益或网站权限。观察到一例疑似钓

图 7　流行域名 Cudmoda 的临时 IP 地址上出现的调试信息

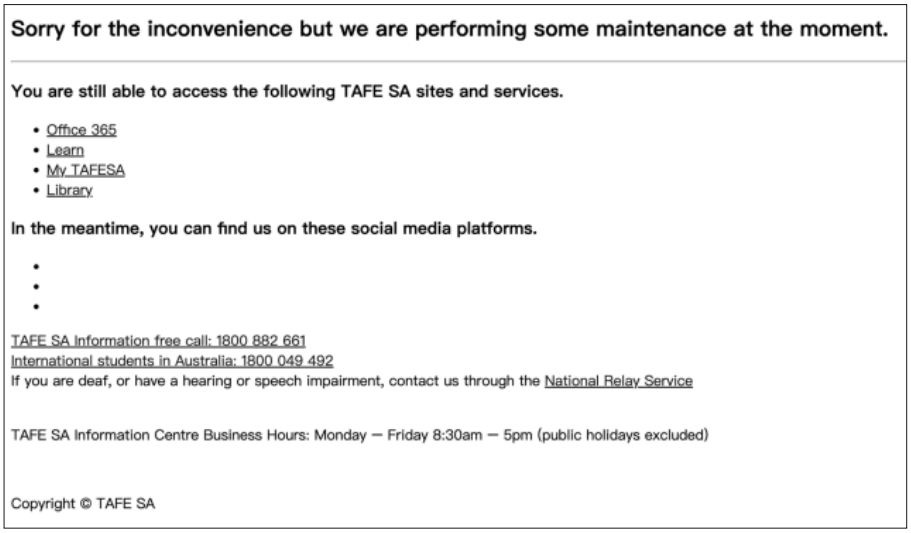


图8　澳大利亚南澳职业技术学院TAFE SA的临时下线说明页面

鱼攻击事件。印度尼西亚巴务巴务府的地方网站（政府行业），该域名本身及www、mail子域名于2024年7月21日5时，IP地址所属自治系统从印度尼西亚地区的AS133800（IDNIC-BIZNETGIO-AS-ID）短暂变更至AS13335（CLOUDFLARENET），其权威服务器同时变更为CloudFlare云平台。此外，位于临时IP地址上的页面并非展示原网站内容，而是显示后台登录页面，要求用户输入账号和密码，如图9所示。这种行为是高度可疑的，攻击者可以通过这种伪造网站登录页面的方式获取到用户的敏感信息，存在隐私泄露等严重风险。

非法内容展示。非法内容展示是指攻击者将域名临时劫持指向非法网站，达到借助正规网站来宣传非法活动的目的。例如，位于伊朗的Momtaznews新闻机构主页（高访问量，Tranco流行度排名约22万位），其IP地址所属自治系统在2024年7月7日8时从伊朗地区的AS43754（ASIATECH）被劫持至云平台AS14061（DIGITALOCEAN-ASN），并且网站页面内容变为非法网站。Madisonwestkiwanis公益俱乐部（高访问量，Tranco流行度排名约12万位）主页的IP地址所属自治系统于7月10日12时从CloudFlare的AS13335被劫持至AS22612（NAMECHEAP-NET），权威服务器厂商从Cloudflare变为Namecheap，页面同样变为非法网站。攻击者吸引用户参与非法活动来谋利，并且损害原网站的声誉。

命中黑名单的可疑行为。域名本身或出现的临时IP地址位于相关的黑名单中，包括IP地址黑名

图9　印度尼西亚巴务巴务政府网站的临时登录页面

单、DNS 黑名单和受已知 DNS 劫持攻击影响的域名名单等。例如，包括教育类产品网站 Smartschool 在内的 22 个网站都被劫持至位于 AS16509（AMAZON-02）的 2 个恶意 IP 地址；位于 DNS 黑名单中的某高访问量非法网站等恶意域名也存在资源记录临时变更现象，疑似被其他恶意团伙劫持。此外，系统观测到了近期针对使用 Squarespace 注册商的加密货币域名劫持攻击[23]，经过与受该攻击影响的域名名单匹配，发现相关机构 dYdX 和 THORChain 域名（高访问量，Tranco 流行度排名约 9 万位和 75 万位）分别于 2024 年 7 月 10 日 0 时和 7 月 26 日 21 时出现资源记录异常变更的现象。

3.4　防御措施与未来工作

算法有效发现了一系列重要域名资源记录异常变更现象，均与域名管理者不当操作甚至是恶意行为密切相关，部分结果命中了近期发生的安全事件。因此，建议域名管理者提高管理流程的自动化程度，减少人为原因造成的配置错误，通过定期自查及时发现管理过程中的问题，避免影响用户的正常访问。此外，建议加强对权威侧域名劫持现象的认知，加固域名管理权限和账号安全，谨慎防范网络钓鱼等攻击。最后，应当对政府、教育等重要行业域名建立权威侧资源记录长期监测机制。本文提出的监测系统和筛选程序将持续运行，未来将设计并实现网站页面，向域名管理者和安全研究者开放，提供数据集查询、域名检测和投诉反馈等功能，在帮助域名管理者快速排查问题的同时为安全研究人员的其他研究工作提供支持，为监管部门及时发现权威侧域名劫持现象提供依据，对可疑的攻击行为进行及时预警和处置。针对存在可疑行为的域名，将与域名的管理组织积极联系，确认域名是否存在被劫持的现象，并根据在反馈结果中提取的行为特征持续优化系统的执行逻辑和运行流程，提高系统筛选的准确性。

4　结束语

针对全球各国政府、教育等重要行业域名和高访问度的流行域名，设计并实现了互联网域名权威侧资源记录监测系统 DomainWatch，长时间、高频次监测了数百万域名的权威侧资源记录，构建可检索的大规模域名资源记录历史数据库。结合系统形成的海量数据集，针对劫持行为隐蔽、短时的特点，提出多维信息关联的资源记录异常变更筛选算法 HijackHound，在一个月的分析周期内发现 896 个重要域名存在资源记录的异常变更现象。经人工验证，导致异常变更的原因包含域名管理者管理不当、钓鱼攻击和非法内容展示等行为。本文提出的系统将持续运行，及时预警域名资源记录的异常变更和可疑的攻击行为，帮助域名管理者排查错误配置，为监管部门及时处置权威侧域名劫持攻击提供依据。

参考文献：

[1] Forbes. Baidu hijacked by cyber army[EB/OL]. 2010

[2] DAGON D, PROVOS N, LEE C P, et al. Corrupted DNS resolution paths: the rise of a malicious resolution authority[C]//Proceedings of the Network and Distributed System Security Symposium. Piscataway: IEEE Press, 2008: 1-15.

[3] WEAVER N, KREIBICH C, PAXSON V. Redirecting DNS for ads and profit[C]//Proceedings of IEEE Symposium on Foundations of Computational Intelligence. Piscataway: IEEE Press, 2011:1-6.

[4] CHUNG T, CHOFFNES D, MISLOVE A. Tunneling for transparency: a large-scale analysis of end-to-end violations in the Internet[C]//Proceedings of the 2016 Internet Measurement Conference. New York: ACM Press, 2016: 199-213.

[5] LIU B J, LU C Y, DUAN H X, et al. Who is answering my queries: understanding and characterizing interception of the DNS resolution path [C]//Proceedings of the Applied Networking Research Workshop. New York: ACM Press, 2019: 1113-1128.

[6] KÜHRER M, HUPPERICH T, BUSHART J, et al. Going wild: Large-scale classification of open DNS resolvers[C]//Proceedings of the 2015 Internet Measurement Conference. New York: ACM Press, 2015: 355-368.

[7] JONES B, FEAMSTER N, PAXSON V, et al. Detecting DNS root manipulation[M]. Cham: Springer International Publishing, 2016

[8] ARENDS R, AUSTEIN R, LARSON M, et al. RFC 4033: DNS security introduction and requirements[EB/OL]. 2005.

[9] EASTLAKE D, ANDREWS M. Domain name system (DNS) cookies [J]. RFC, 2016, 7873: 1-25.

[10] HU Z, ZHU L, HEIDEMANN J S, et al. Specification for DNS over transport layer security (TLS)[J]. RFC, 2016, 7858: 1-19.

[11] KREBS B. A deep dive on the recent widespread DNS hijacking attacks[EB/OL]. 2019.

[12] BENJAMIN B. Investigating DNS hijacking through high frequency measurements[D]. California: University of California, San Diego, 2016.

[13] AKIWATE G, SOMMESE R, JONKER M, et al. Retroactive identification of targeted DNS infrastructure hijacking[C]//Proceedings of the 22nd ACM Internet Measurement Conference. New York: ACM Press, 2022: 14-32.

[14] HOUSER R, HAO S, LI Z, et al. A comprehensive measurement-based investigation of DNS hijacking[C]//Proceedings of the 2021 40th Inter-

national Symposium on Reliable Distributed Systems (SRDS). Piscataway: IEEE Press, 2021: 210-221.
[15] RIJSWIJK-DEIJ R V, JONKER M, SPEROTTO A, et al. A high-performance, scalable infrastructure for large-scale active DNS measurements[J]. IEEE Journal on Selected Areas in Communications, 2016, 34(6): 1877-1888.
[16] KOUNTOURAS A, KINTIS P, LEVER C, et al. Enabling network security through active DNS datasets[M. Cham: Springer International Publishing, 2016.
[17] Rapid7 Labs. Open Data[EB/OL]. 2019.
[18] POCHAT V L, VAN GOETHEM T, TAJALIZADEHKHOOB S, et al. Tranco: a research-oriented top sites ranking hardened against manipulation[J]. arXiv Preprint, arXiv: 1806.01156, 2018.
[19] IZHIKEVICH L, AKIWATE G, BERGER B, et al. ZDNS: a fast DNS toolkit for Internet measurement[C]//Proceedings of the 22nd ACM Internet Measurement Conference. New York: ACM Press, 2022: 33-43.
[20] T145. Black mirror [EB/OL].(2021) [2024-10-22].
[21] Github. 0xngmi[EB/OL]. (2024)[2024-10-22].
[22] ZIRNGIBL J, DEUSCH S, SATTLER P, et al. Domain parking: largely present, rarely considered! [C]//Proceedings of Traffic Monitoring and Analysis. Berlin: Springer, 2022: 1-9.
[23] BILL T. DNS hijacks target crypto platforms registered with Squarespace[EB/OL].(2024)[2024-10-22].

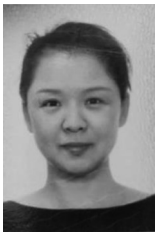
[作者简介]

孙俊哲（2002–），男，北京人，清华大学硕士生，主要研究方向为网络安全和互联网测量。

陆超逸（1995–），男，四川乐山人，博士，清华大学在站博士后，主要研究方向为网络安全、互联网测量。

刘保君（1994–），男，安徽宿州人，博士，清华大学助理教授、博士生导师，主要研究方向为网络安全、网络测量、网络犯罪检测等。

段海新（1972–），男，山东济宁人，博士，清华大学教授、博士生导师，主要研究方向为网络和系统安全。



孙东红（1974–），女，黑龙江哈尔滨人，博士，清华大学副研究员，主要研究方向为网络与信息安全。