# 面向教育网的域名基础设施安全状态测量与分析

刘保君

2023年11月28日

# 报告主要内容

- 教育网域名运行安全现状测量研究
  - 整体安全属性
  - DNSSEC部署应用
  - 域名基础设施集中化
- 新兴热点域名安全机制测量研究
  - 加密DNS协议
  - 防护型DNS（Protective DNS）服务
- 教育网安全DNS服务介绍
  - 服务基本情况
  - 服务特色

# 教育网域名运行安全现状

## 整体安全属性测量

# 域名系统安全测量指标

## ◆ 安全指标设计（域名权威服务器侧）

◇各高校域名系统的**建设时间不同**、**管理能力不同**等

◇需要专门设计安全指标用于测试

◇指标主要考虑**配置**与**管理**方面带来的安全风险

| 类别 | 指标 | 类别 | 指标 |
| --- | --- | --- | --- |
| 域名权威服务器<br>**基础配置**特性 | 是否具有备份权威服务器 | 域名权威服务器<br>**安全风险**评估 | 域名权威服务器地理位置<br>是否位于境外 |
| | 是否满足地理位置分布与<br>网络环境分布的多样性 | | 是否支持EDNS、是否正确<br>支持DNS COOKIE、DNSSEC |
| | 是否支持IPv6解析与访问 | | 是否受典型已知<br>域名攻击影响 |

# 域名系统安全测量情况

- 测量时间
  - 2023年2月——2023年3月
- 测量对象
  - 2023年2月CERNET会员活跃域名，共包含1960个门户网站域名。
    - 存在49个域名目前已经无法访问到相关网站
    - 存在67个域名虽然能访问网站，但是由于其配置问题导致无法找到实际运行的权威服务器
- 测量方法
  - 对于大部分指标，采用主动测量的方法，主动发包并解析返回结果
  - 对于典型攻击影响评估，采用主动测量的方法，尽可能保证评估无害化

# 域名系统基础配置测量情况

## ◆ NS备份与分布

◇ 教育系统网站权威服务器的冗余性实现得较好，可以有效防止单点故障问题。

◇ 但是大部分域名NS分布都位于**同一省份**。

## ◆ IPv6解析与访问支持

◇ **91.05%**教育系统网站都存在可供访问的IPv6地址

◇ 其中仅有**66.92%的网站是链路可达的**。

教育系统网站 NS 部署情况

| 类别 | 计数 | 占比 |
|---|---|---|
| 具有备份 NS 的域名 | 1374 | 74.55% |
| 不具有备份 NS 的域名 | 469 | 25.45% |
| NS 分布具有多样性的域名 | 198 | 10.74% |
| NS 分布不具有多样性的域名 | 1645 | 89.26% |

# 域名系统安全风险评估情况

## DNS安全性协议支持

- 98.21%的域名都支持EDNS
- 67.23%的域名会返回Server Cookie，其中几乎所有的域名都按照RFC的建议将时间戳加入Server Cookie中，从而实现了动态Cookie
- 仅有2.06%的域名配置了DNSSEC

## 典型DNS攻击威胁情况

- 少量NS存在**区域文件任意传输风险**
- 存在**部分子域名易受到劫持**的风险

教育系统网站受典型 DNS 攻击威胁情况

| 攻击名称 | 计数 | 占比 |
| --- | --- | --- |
| 非授权的区域传输攻击 | 16 | 0.87% |
| 匿名动态更新攻击 | 0 | 0.00% |
| 子域名劫持风险 | 105 | 5.70% |

# 域名权威服务器的安全运行建议

- 思考和建议
  - 更新权威服务器的软件版本，并正确支持安全性协议
    - 正确支持EDNS机制，它是其他安全协议的基础
    - 可选部署相对轻量的DNS Cookie机制
    - 大力推广DNSSEC机制的支持
  - **正确规范权限问题，关注重要操作的权限控制**
  - **及时更新各项记录，保持对权威服务器的维护**

# 教育网域名运行安全现状

DNSSEC部署

# 教育网域名DNSSEC部署规模

## ◆ edu. cn域名DNSSEC部署规模变化

◇ 测量时间：**2023年5月、11月（教育网于5月底开展DNS安全技术培训）**

| 时间 | 测试域名数量 | 有意愿部署DNSSEC的域名数量 | 正确部署DNSSEC的域名数量 | 正确部署DNSSEC的域名比例 |
|---|---|---|---|---|
| 2023. 05 | 1839 | 38 | 37 | 2. 01% |
| 2023. 11 | 1839 | 49 | 48 | 2. 61% ▲ |

## ◆ 主要结论

◇ edu. cn域名部署DNSSEC的**规模仍然较低**

◇ 在开展技术培训后，**edu. cn域名部署DNSSEC的规模有少量增长**

# 教育网域名DNSSEC部署问题

- 问题一：使用无效的数字签名
  - 某edu.cn域名使用DSA算法（算法代码3），**导致签名无法通过验证**
  - 同一域名，在5月测试时**签名已过期**；该问题近期已得到修复
- 问题二：使用不推荐的密钥算法
  - 如RSAMD5、DSA、RSASHA1等
  - 算法强度偏弱或已被淘汰，**存在密钥被攻破的潜在风险**

| 正确部署DNSSEC的域名数量 | 使用高强度加密算法的域名数量 | 使用高强度加密算法的比例 | 未使用高强度加密算法的比例 |
|---|---|---|---|
| 48 | 29 | 60.42% | 39.58% |

# 教育网域名DNSSEC部署问题

- DNSSEC密钥算法推荐列表

RFC 8624: https://www.rfc-editor.org/rfc/rfc8624.html

| Number | Mnemonics | DNSSEC Signing | DNSSEC Validation |
|---|---|---|---|
| 1 | RSAMD5 | MUST NOT | MUST NOT |
| 3 | DSA | MUST NOT | MUST NOT |
| 5 | RSASHA1 | NOT RECOMMENDED | MUST |
| 6 | DSA-NSEC3-SHA1 | MUST NOT | MUST NOT |
| 7 | RSASHA1-NSEC3-SHA1 | NOT RECOMMENDED | MUST |
| 8 | RSASHA256 | MUST | MUST |
| 10 | RSASHA512 | NOT RECOMMENDED | MUST |
| 12 | ECC-GOST | MUST NOT | MAY |
| 13 | ECDSAP256SHA256 | MUST | MUST |
| 14 | ECDSAP384SHA384 | MAY | RECOMMENDED |
| 15 | ED25519 | RECOMMENDED | RECOMMENDED |
| 16 | ED448 | MAY | RECOMMENDED |

应当避免使用红框标识的淘汰或不推荐算法

# 教育网DNSSEC部署用户调查

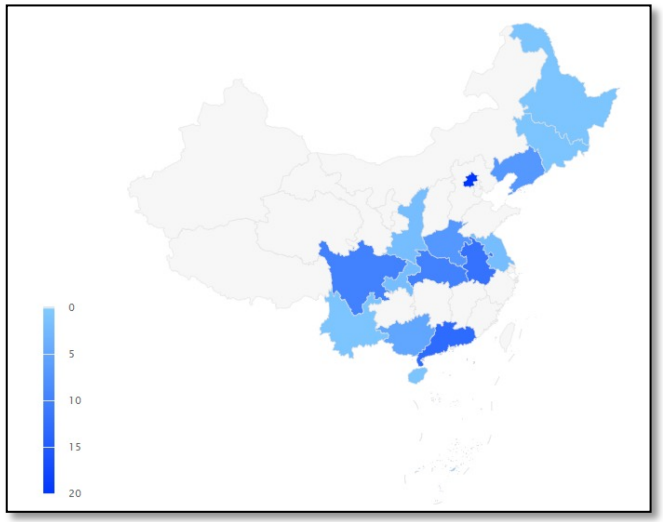
## ◆ 问卷发布情况

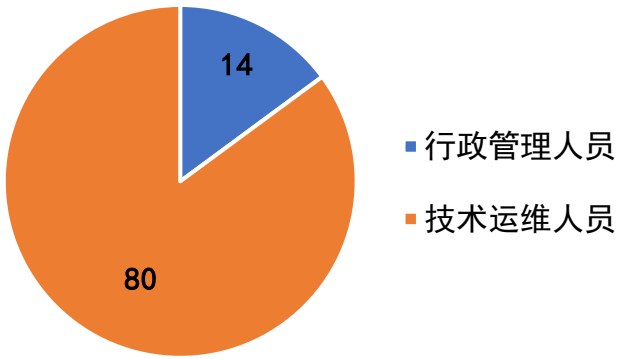
- ◇ **调查目的：**调研“edu.cn”DNSSEC的部署情况
- ◇ **调研时间：**2023年5月25日CERNET用户DNS安全技术培训会
- ◇ **调研对象：**CERNET用户高校的网络管理/技术人员
- ◇ **调研方法：**线上+线下 结合的问卷调查
- ◇ **调研内容：**
  - 对DNSSEC概念以及重要性的认识
  - 针对DNSSEC的部署现状和原因

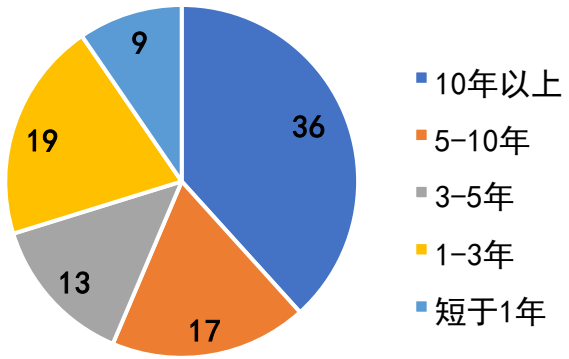
# 教育网DNSSEC部署用户调查

## ◆ 问卷参与者基本信息

- ◇ **问卷数量：共收集94份问卷**
- ◇ **人员分布：参与者分散在全国各地区，共涉及16个省**
- ◇ **人员类型：行政管理人员占比14. 89%，技术运维人员占比85. 11%**
- ◇ **从业年限：38. 3%的人从事教育网安全相关工作超过10年**



# 教育网DNSSEC部署用户调查结果

## ◆ 问题一：对DNSSEC概念的认识与理解

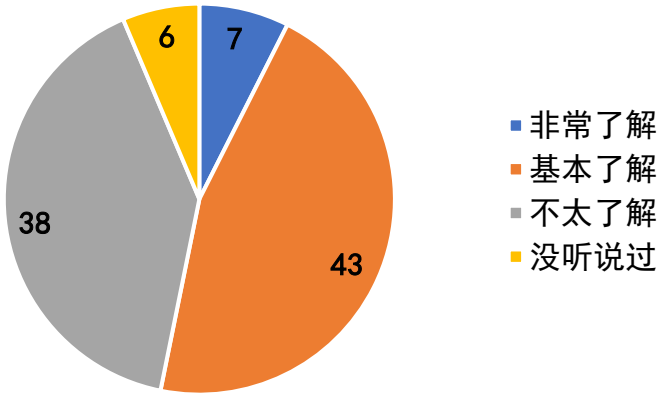
### ◇ 对于DNSSEC的了解程度整体较低

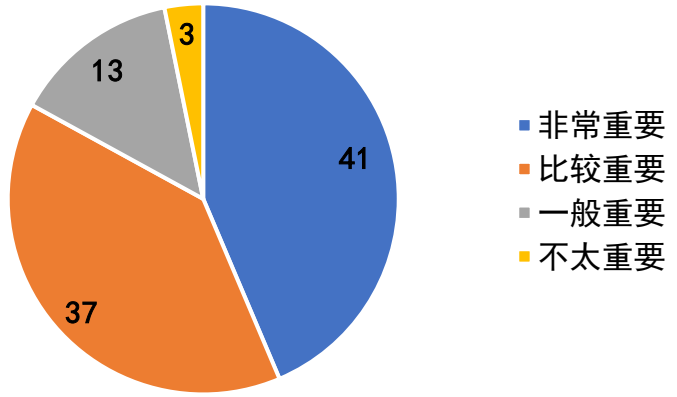
- 40.43%的参与者不太了解，仅听说过DNSSEC这个词

◇ 大部分参与者对于DNSSEC的**重要性持肯定态度**

- 43.62%的参与者认为DNSSEC非常重要，能够显著提升教育网的安全性

◇约20%左右的参与者**对DNSSEC的作用和技术细节存在疑虑和不了解**



# 教育网DNSSEC部署用户调查结果

## ◆ 问题二：DNSSEC的部署现状和原因

### ◇ 大多数参与者所在教育机构**尚未部署DNSSEC**

- 7.45%参与者所在单位已经部署了DNSSEC；74.47%尚未部署DNSSEC

### ◇ 大部分机构**缺乏DNSSEC相关网络安全培训**

- 仅有3.19%的参与者所在机构进行过针对DNSSEC的安全培训

### ◇ **任务尚不急迫是导致没有部署DNSSEC的最主要原因**

- 其他原因包括：**部署复杂度高、缺乏专业人员、时间和预算限制、缺乏上级批示**

# 教育网DNSSEC部署思考

## ◆ 思考和建议

### ◇ 定期开展DNSSEC相关网络安全技术培训

- 提升技术人员对于DNSSEC重要性的认识
- 培养技术人员对于DNSSEC部署的能力
- 加强技术人员对DNSSEC密钥维护和更新的意识

### ◇ 提供有效的针对DNSSEC部署的技术指导手册

### ◇ **通过官方政策的方式加速DNSSEC的部署范围和速度**

# 教育网域名运行安全现状

域名基础设施集中化

# 域名基础设施集中化

## ◆ 研究背景

◇ 尽管DNS是一种**分布式**的解析架构，但国外的研究表明，用户使用的递归解析器和权威域名服务器存在**高度集中化**趋势

◇ 集中化表现为**多个用户共用**同一递归解析器，以及多个网络管理员将域名托管在同一权威服务器上

## ◆集中化带来的问题

◇ **单点故障：**关键设施发生问题将影响**大片域名系统**

◇ **性能瓶颈：**用户和流量增加，无法有效处理**高负载**

◇ **业务垄断：**限制了市场竞争，影响**公平性和创新**

# 基于广告投放测量递归解析器集中化现象

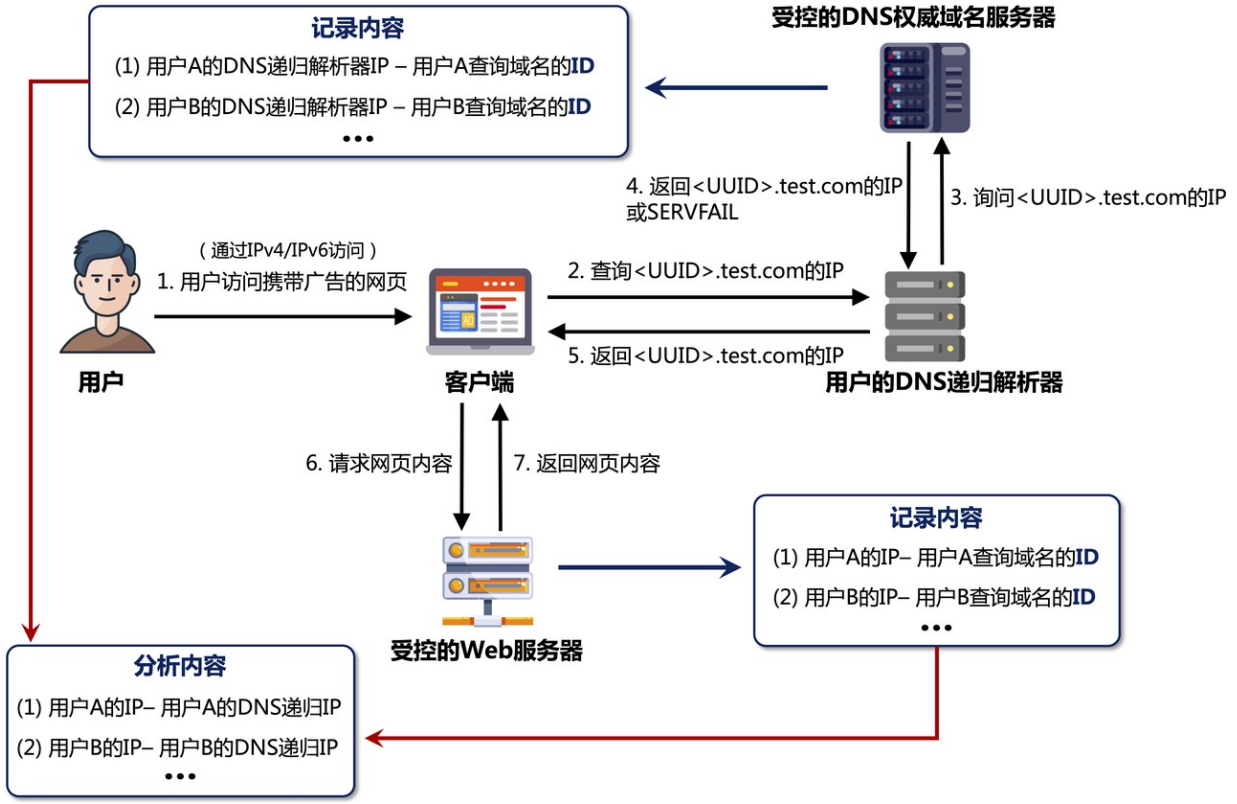
## ◆ 测量方法

◇ 自行配置DNS权威域名服务器和Web服务器进行**数据收集**

◇ 编写广告，用户触发广告便向权威域名服务器**发起查询**

◇ 发布广告并开展**主动探测**，一共收集345539条广告流量

◇ 广告流量**遍布全国**所有省市，包括港澳台地区



# 递归解析器集中化测量结果

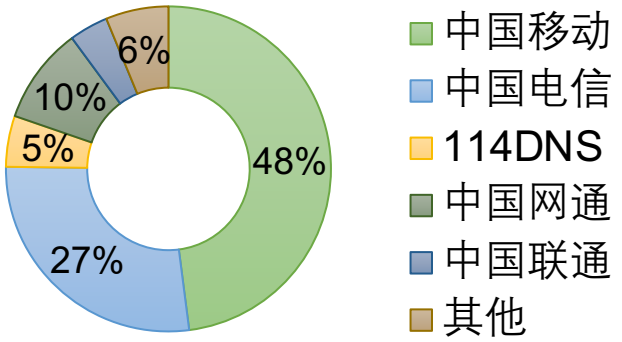
## ◆ 国内用户使用的递归解析器呈现集中化现象

### ◇ 我国用户配置递归解析器

- **有90.35%选用ISP为用户分配的解析器而非知名公共解析器**
- 有84.61%与其IP在同一自治域下
- 有99.22%使用着国内提供的递归解析器

### ◇ 同时，针对使用ISP提供解析器的人群

- 有82.16%能够被分配到在同一省市下的解析器
- 有99.90%能够使用国内提供的递归解析器




## ◆ 总结

### ◇ **递归解析器的集中化表现在ISP为用户分配的递归解析器**

### ◇ **ISP分配解析器时尽可能的考虑与用户之间的物理距离，从而提供更好的服务**

# 基于主动收集测量权威域名服务器集中化现象

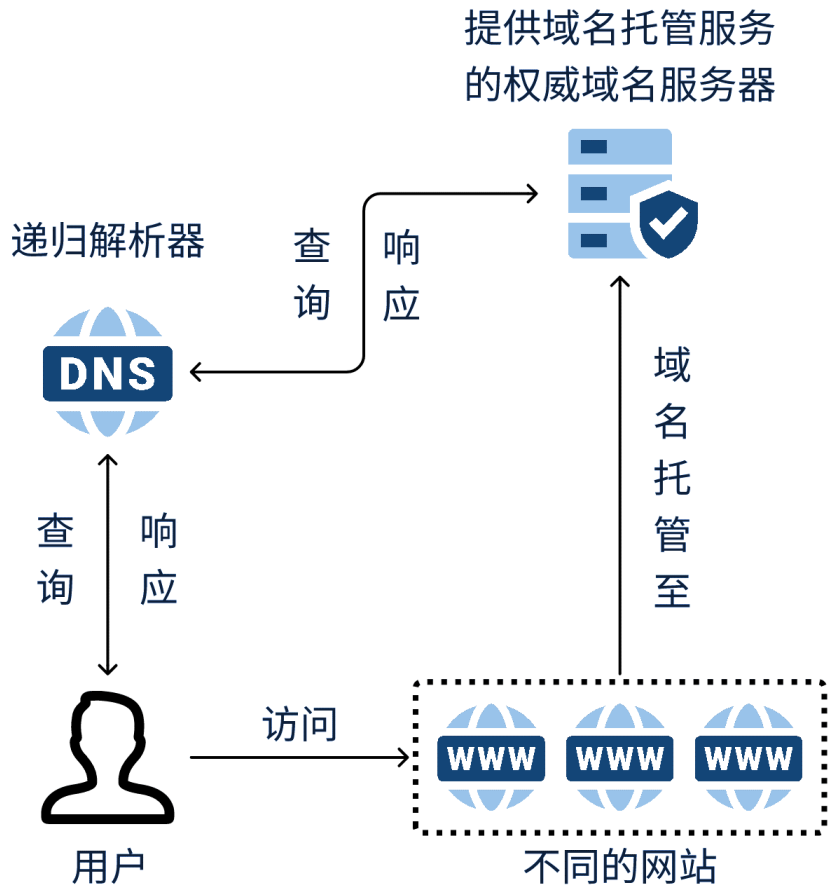
## ◆ 测量方法

◇收集以.cn作为顶级域的二级域名作为数据集。

◇向递归解析器查询该域名的NS记录，即这些域名的**权威服务器**。

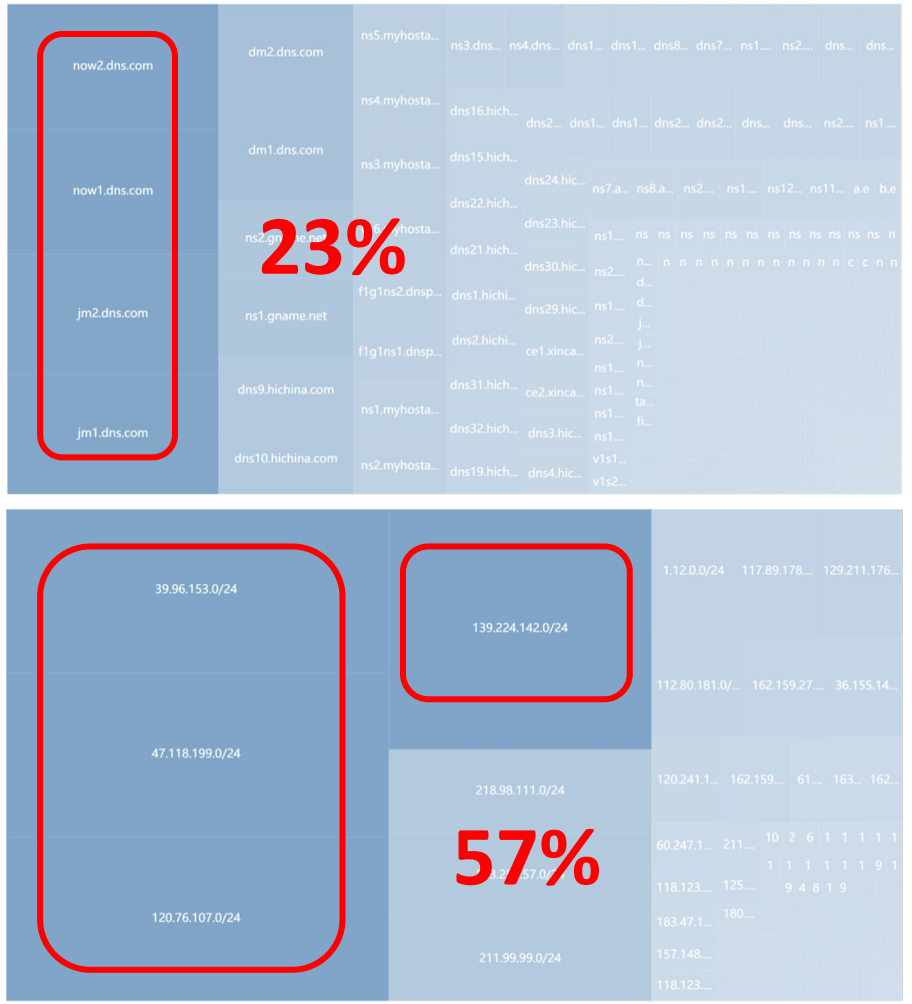
◇向递归解析器查询这些权威服务器的A记录，即其**IP地址**。

◇分析这些权威服务器的域名和其IP**托管.cn域名的数量**。



# 权威域名服务器集中化测量结果

- .cn托管的权威域名服务器存在集中化趋势
  - 从权威本身的**域名**来看：
    - 主要集中在now2.dns.com、now1.dns.com；jm2.dns.com、 jm2.dns.com
  - 从权威所在的**IP网段**来看：
    - 主要集中在39.96.153.33、47.118.199.193、120.76.107.33、139.224.142.97
    - 这些网段均来自于**阿里云**
- 总结
  - **域名集中托管至阿里云，其对自身服务器的性能、灾备能力、防御措施等采取更严的要求。**



# 新型热点域名安全机制测量

加密DNS协议

# 加密DNS成为缓解域名系统威胁的新兴技术

- 什么是加密DNS？
  - 通过**加密的通信信道**传输域名报文，提供域名消息的保密性和身份认证服务
- 它们解决什么问题？
  - 明文传输的传统域名协议所引发的**安全和隐私**问题（中间人监听、篡改）
- 部署在什么位置？
  - 终端用户和递归解析服务器（**已标准化**）
  - 递归解析服务器和权威域名服务器（**标准化进程中**）
- 标准化的情况？
  - DNS over TLS（2016年，RFC 7858）
  - DNS over HTTPS（2018年，RFC 8484）
  - DNS over QUIC（2022年，RFC 9250）

# 近年全球加密DNS服务部署增长幅度放缓

## ◆ 有多少加密DNS服务在运行？

◇ DoT和DoH递归解析器数量小幅降低，DoQ递归解析器数量大幅增长

| 年份 | DoT | DoH | DoQ |
|---|---|---|---|
| 2022年7月 | 21029 | 10944 | 1978 |
| **2023年9月** | 17291 ▼ | 8951 ▼ | 4027 ▲ |

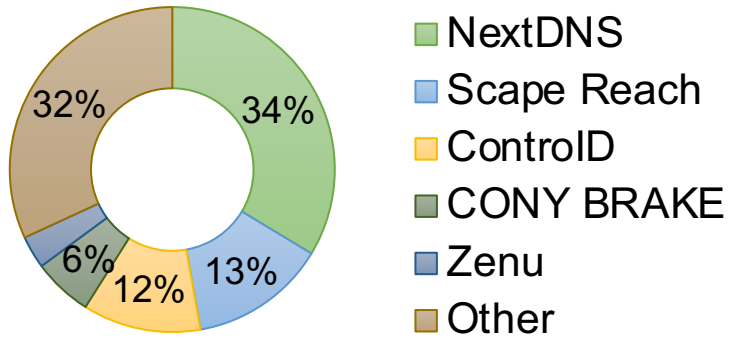
## ◆加密DNS服务的不当配置普遍存在

◇ 加密DNS遭受证书生态系统弱点的威胁（私钥泄漏、证书过期、证书颁发机构妥协）

◇ 30%左右的加密DNS服务器配备无效证书

# 加密DNS生态系统呈现严重集中化现象

- 谁在运行加密DNS服务器？
  - 全球**超过3000个**组织运营加密DNS服务器（Google、Cloudflare、OpenDNS）
  - Firefox的加密DNS合作伙伴NextDNS
    部署了大约30%的加密DNS服务器




- 集中化现象阻碍加密DNS发展
  - 不道德的供应商可更容易地获取用户域名解析流量，来进行**广告投放和数据交易**
  - 50%左右的加密DNS服务器属于5个大型DNS厂商

# 新型热点域名安全机制测量

防护型DNS服务

# 防护型DNS服务有效阻止恶意域名的解析

- 域名解析是网络攻击生命周期的必须过程
  - 超过**91%的恶意软件**使用DNS执行攻击行为


恶意软件

钓鱼攻击


数据窃取


DNS隧道

- 防护型DNS得到广泛部署


美国

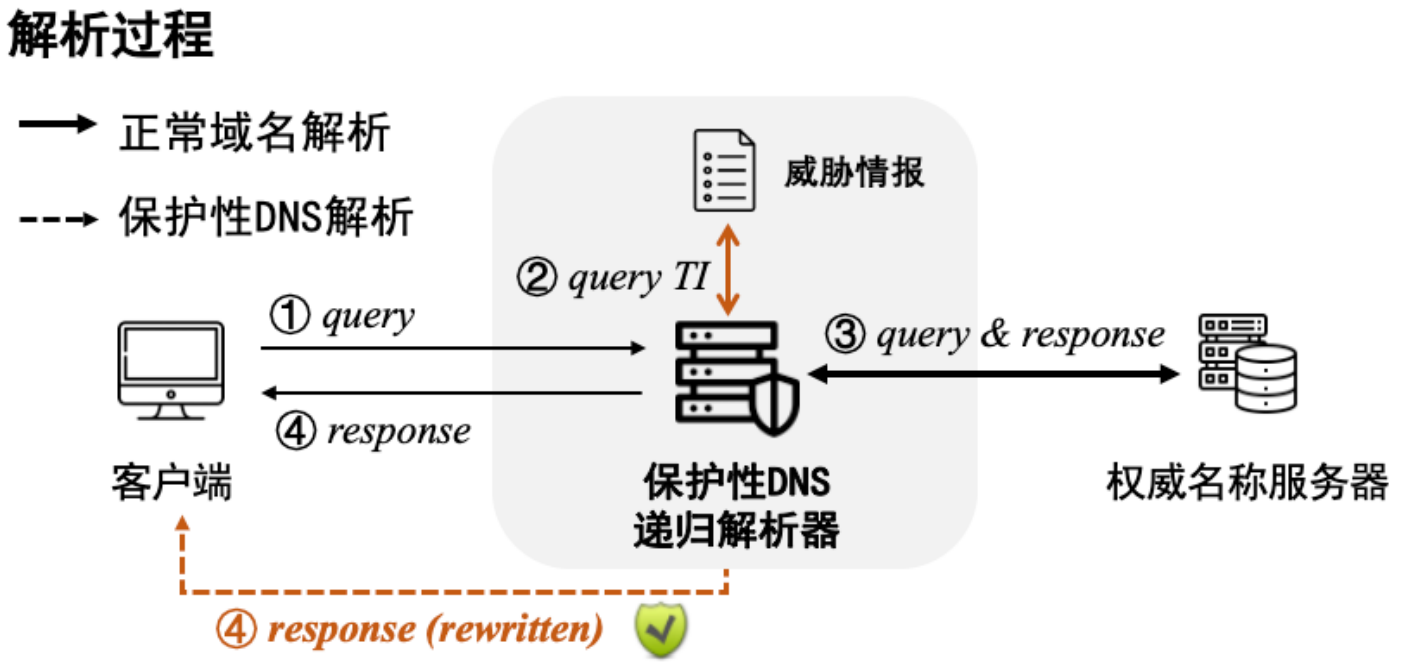

加拿大


欧盟

*https://umbrella.cisco.com/blog/dns-security-your-new-secret-weapon-in-your-fight-against-cybercrime*

# 防护型DNS服务有效阻止恶意域名的解析

- 防护型DNS服务部署于递归服务器上，阻断恶意域名解析
  - 将恶意域名的解析结果引导至**可控且安全**的服务器

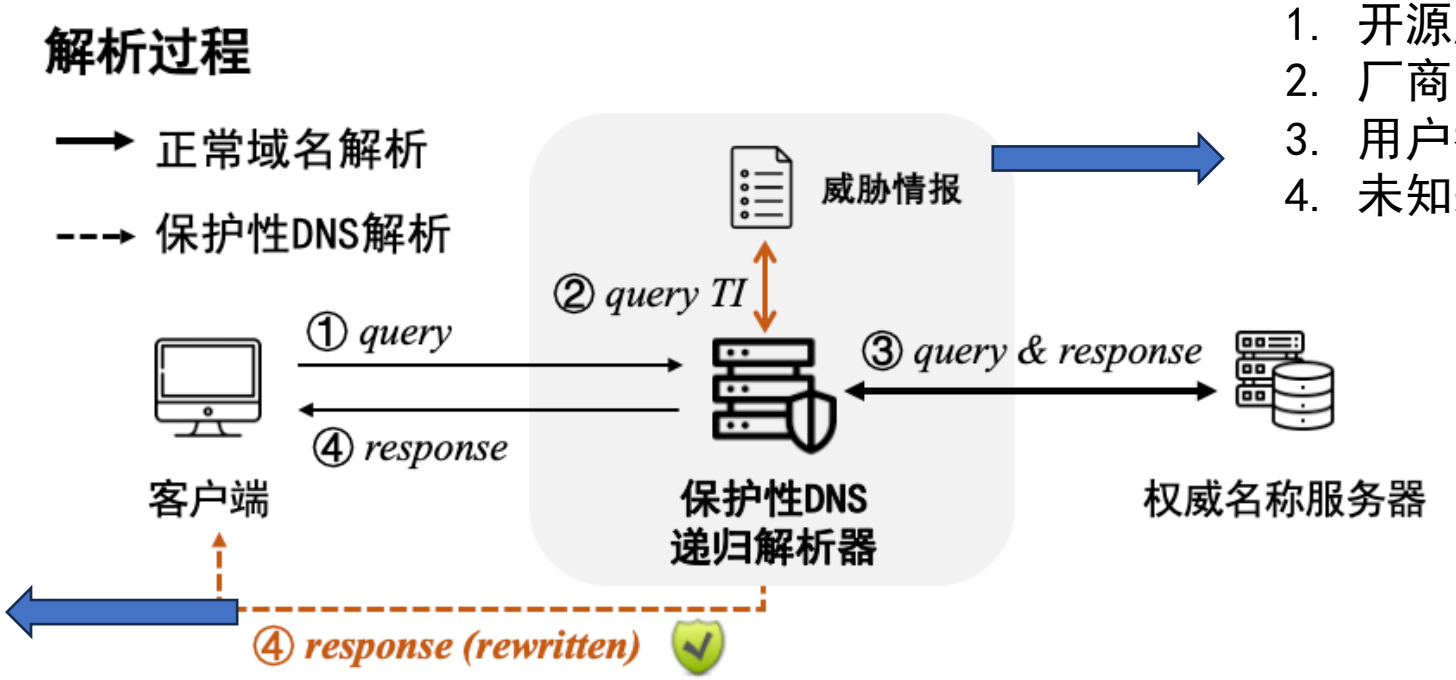


# 防护型DNS服务有效阻止恶意域名的解析

- 防护型DNS服务部署于递归服务器上，阻断恶意域名解析
  - 将恶意域名的解析结果引导至**可控且安全**的服务器
  - 关键组件：**恶意域名列表与阻断策略**

**恶意域名列表**

1. 开源威胁情报
2. 厂商自己维护
3. 用户举报投诉
4. 未知来源

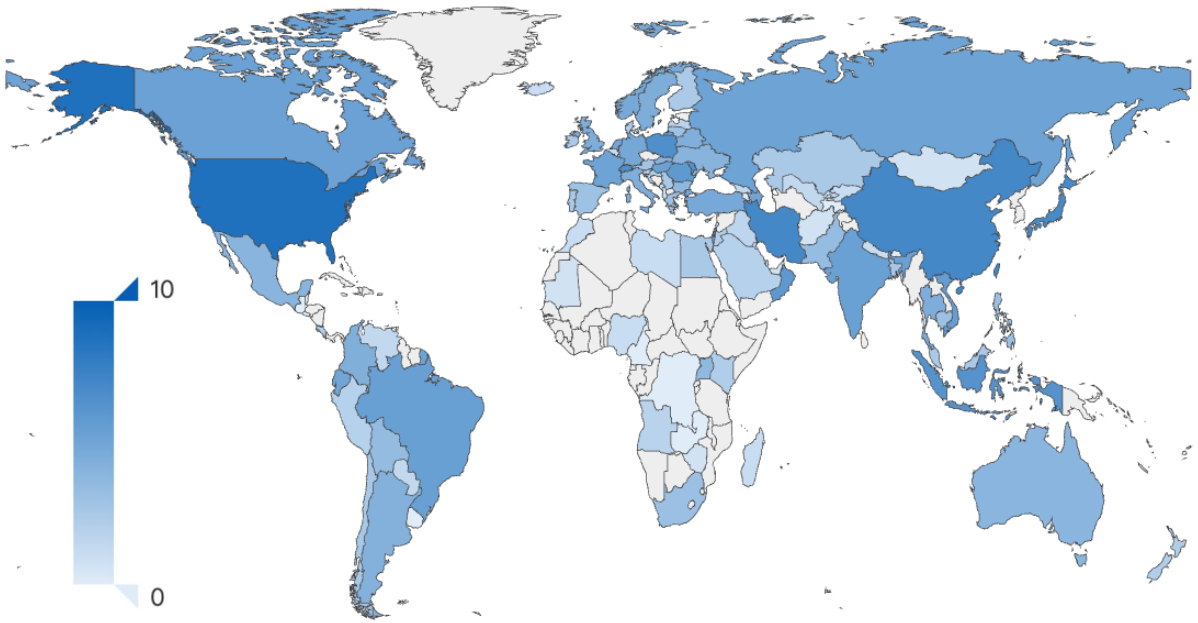



**阻断策略**

1. 特殊用途的IP地址，0.0.0.0
2. 安全IP地址
3. 安全CNAME域名
4. Response Code，NXDomain
5. 空解析响应数据包

# 防护型DNS服务的部署现状

- 保护性DNS服务部署广泛
  - 通过主动测量分析，我们共发现17, 601 (9. 08%) 保护性DNS服务器
  - 保护性DNS服务的部署广泛分布于全世界




| 国家 | 防护性DNS数量(%) |
|---|---|
| 美国 | 6,296 (35.8%) |
| 伊朗 | 1,225 (7.0%) |
| 中国 | 1,205 (6.8%) |
| 日本 | 1,056 (6.0%) |
| 瑞士 | 804 (4.6%) |
| 共分布于117个国家 | |

# 教育网安全DNS推广

服务基本情况及特色

# 教育网内域名解析现状

## ◆ 域名服务方案

◇ 各高校主要通过三种方式为校园网用户提供域名解析服务，即自建域名解析服务、使用外部商业域名解析服务，以及直接采用当地电信运营商提供的域名解析服务

## ◆目前处理方案的问题

◇ 服务安全性：自建和运营商提供的域名解析服务，普遍存在软件更新不及时、配置不当等问题，缺少对最新安全域名协议的支持，容易产生安全隐患

◇ 服务性能：位于教育网外部的域名解析服务，对于教育网内域名解析调度缺乏优化，容易影响网络性能、形成资源访问瓶颈

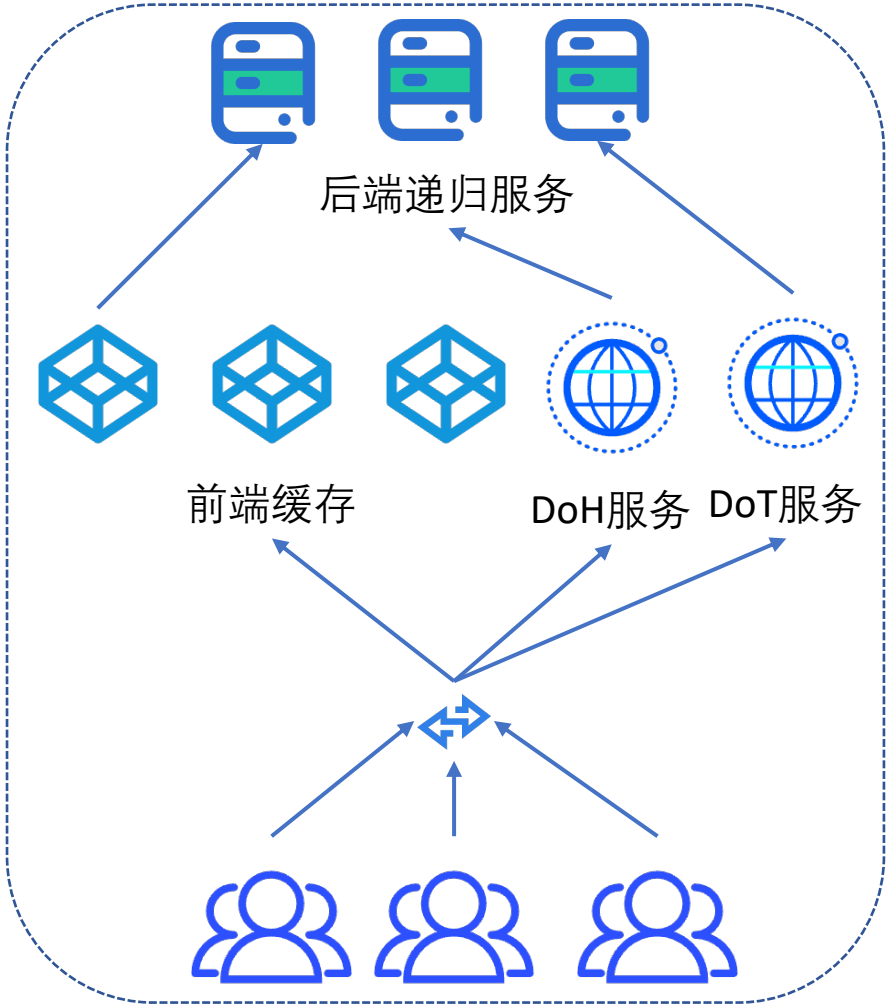
# 教育网科研试验用途安全DNS 101.7.7.7

## ◆服务地址

- ◇ IPv4: **101.7.7.7**
- ◇ IPv6: 2001:DA8:7:0:101:7:7:7
- ◇ DoH: doh.cernet.edu.cn
- ◇ DoT(介绍主页): dot.cernet.edu.cn

## ◆服务架构

- ◇ CERNET公益域名系统由清华大学-奇安信联合研究中心与114 DNS 合作研发
- ◇采用业界标准的前后端负载均衡架构以及Anycast满足高负载下服务需求
- ◇使用标准化商业实现搭建DoH/T服务，提供更安全的DNS解析服务




CERNET-DNS架构示意

# 感谢您对提升教育网安全性做出的贡献！

- 关于DNS cookie安全机制的问卷调查
  - 一种**轻量级、易部署**的新型DNS安全机制，由RFC 7873标准化
  - 在教育网得到了一定程度的部署：超过60%的域名权威服务器支持
- 我们希望了解您对DNS cookie安全机制的看法
  - 调查结果仅作学术研究用途，感谢您协助我们推动该机制在教育网中的部署
  - 2-3分钟即可完成

# 谢谢

2023年11月28日