清华大学
Tsinghua University

2020年CERNET学术年会
网络安全论坛

CERNET DNS安全服务与威胁情报分析

报告人：刘保君

清华大学网络研究院

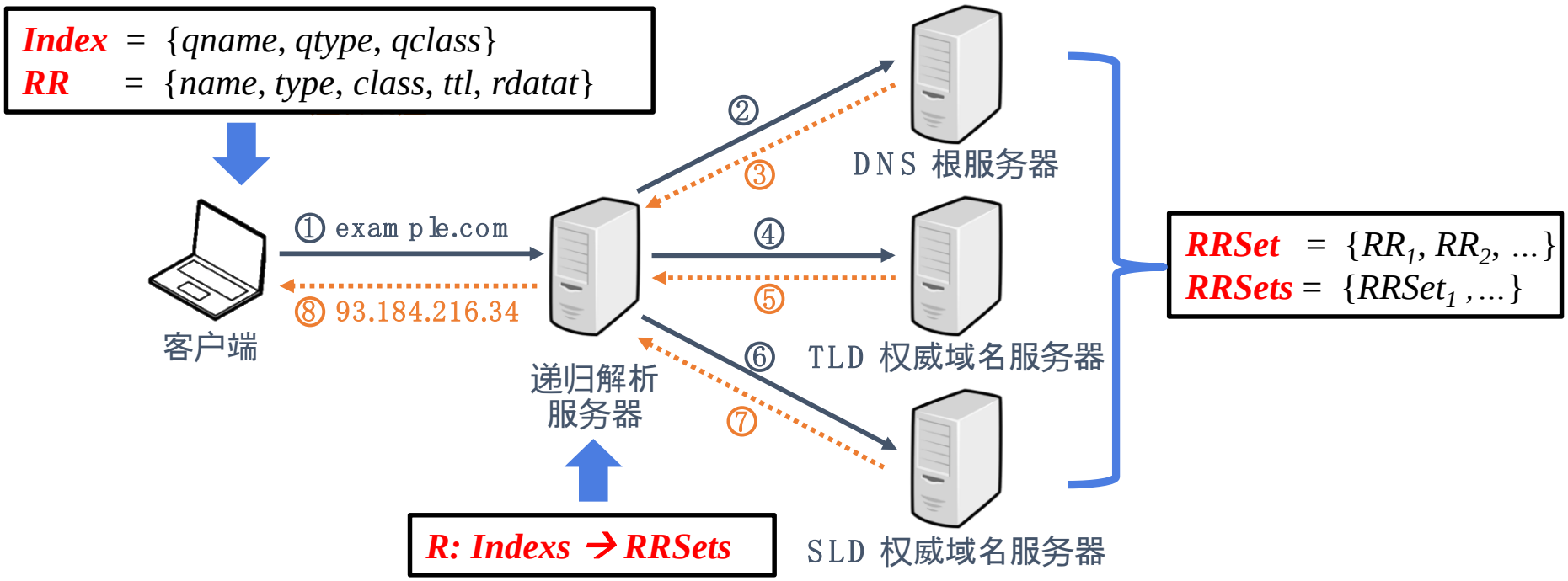
2020年12月1日

个人简介

- 清华大学计算机系，博士
  - 指导教师：刘莹老师，段海新老师
- 清华大学网络研究院，博士后
  - 合作导师：段海新老师
- 研究方向：互联网基础设施安全
  - 域名系统：[NDSS '21] [USENIX Security '20] [IMC '19] [NDSS '19] [USENIX Security '18] [CCS '17]
  - 网络测量：[USENIX Security '21] [CCS '20] [S&P '19] [IMC '19]
- 网站主页：https://www.liubaojun.org
- 邮箱地址：lbj@mail.tsinghua.edu.cn

域名系统：结构极其简单

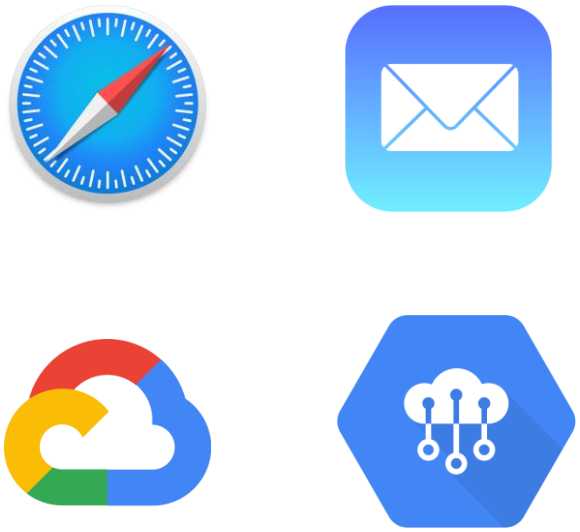
- 域名解析过程，通常集中交付于“递归解析服务器”

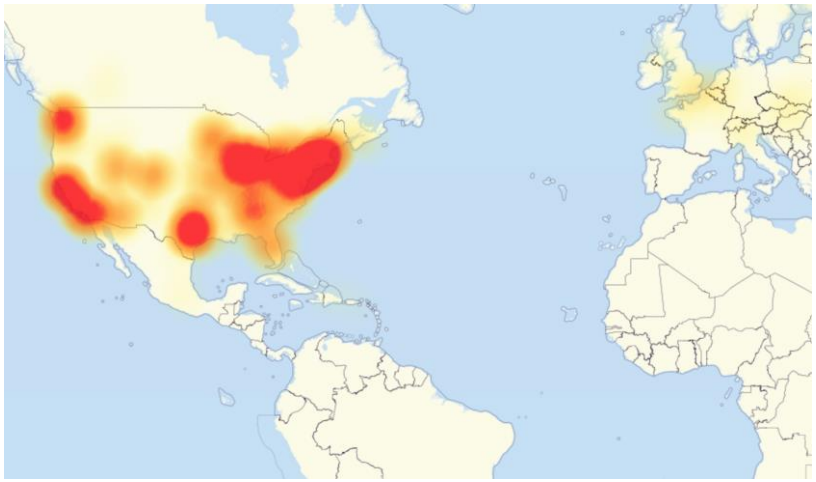


域名应用　　域名解析　　域名空间

域名系统：应用极其广泛

- 域名解析服务的正常运行，是绝大多数互联网上层应用获取网络资源的前提
- 域名系统一旦发生故障，其后果与直接中断网络服务无异



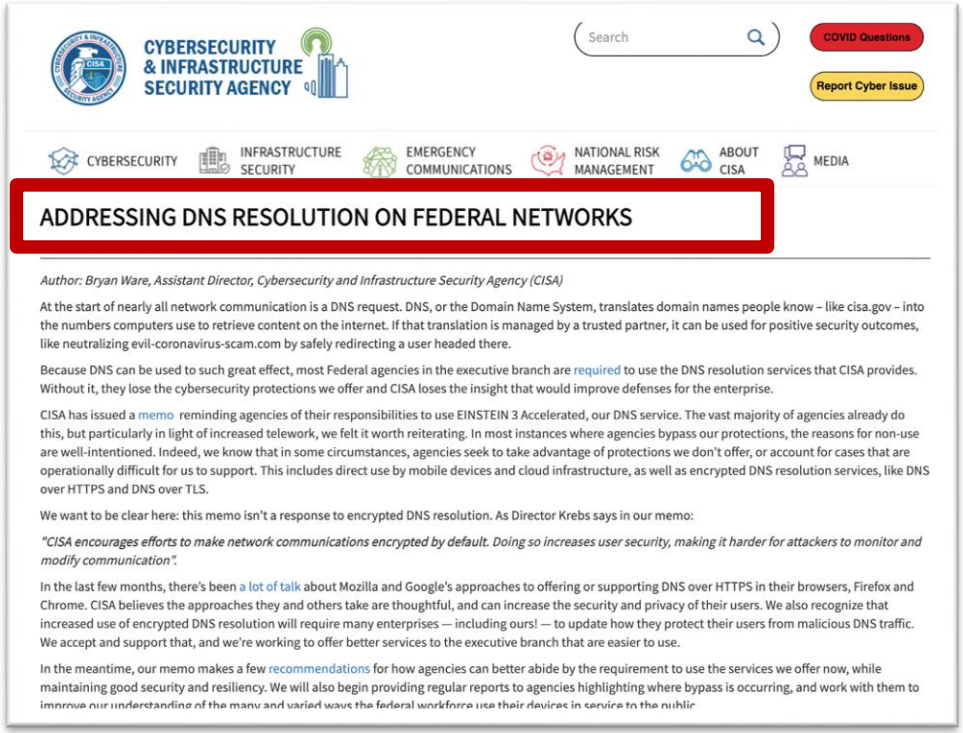


域名解析是绝大多数网络活动的起点

2016年，Dyn DoS攻击事件

国家安全战略愈发重视域名系统的作用

- 美国：EINSTEIN 3 Accelerated (E3A) 计划
- 加拿大：CIRA加拿大盾项目
- 英国，澳大利亚：五年网络安全战略规划



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

COVID Questions

Report Cyber Issue

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

ADDRESSING DNS RESOLUTION ON FEDERAL NETWORKS

Author: Bryan Ware, Assistant Director, Cybersecurity and Infrastructure Security Agency (CISA)

At the start of nearly all network communication is a DNS request. DNS, or the Domain Name System, translates domain names people know – like cisa.gov – into the numbers computers use to retrieve content on the internet. If that translation is managed by a trusted partner, it can be used for positive security outcomes, like neutralizing evil-coronavirus-scam.com by safely redirecting a user headed there.

Because DNS can be used to such great effect, most Federal agencies in the executive branch are required to use the DNS resolution services that CISA provides. Without it, they lose the cybersecurity protections we offer and CISA loses the insight that would improve defenses for the enterprise.

CISA has issued a memo reminding agencies of their responsibilities to use EINSTEIN 3 Accelerated, our DNS service. The vast majority of agencies already do this, but particularly in light of increased telework, we felt it worth reiterating. In most instances where agencies bypass our protections, the reasons for non-use are well-intentioned. Indeed, we know that in some circumstances, agencies seek to take advantage of protections we don't offer, or account for cases that are operationally difficult for us to support. This includes direct use by mobile devices and cloud infrastructure, as well as encrypted DNS resolution services, like DNS over HTTPS and DNS over TLS.

We want to be clear here: this memo isn't a response to encrypted DNS resolution. As Director Krebs says in our memo:

"CISA encourages efforts to make network communications encrypted by default. Doing so increases user security, making it harder for attackers to monitor and modify communication".

In the last few months, there's been a lot of talk about Mozilla and Google's approaches to offering or supporting DNS over HTTPS in their browsers, Firefox and Chrome. CISA believes the approaches they and others take are thoughtful, and can increase the security and privacy of their users. We also recognize that increased use of encrypted DNS resolution will require many enterprises — including ours! — to update how they protect their users from malicious DNS traffic. We accept and support that, and we're working to offer better services to the executive branch that are easier to use.

In the meantime, our memo makes a few recommendations for how agencies can better abide by the requirement to use the services we offer now, while maintaining good security and resiliency. We will also begin providing regular reports to agencies highlighting where bypass is occurring, and work with them to improve our understanding of the many and varied ways the federal workforce use their devices in service to the public

美国国土安全局 E3A计划

域名系统，一直是学术研究热点

- 会议列表：网络安全领域四大顶会 + 网络测量领域顶会
- 根据近十年来录用论文，汇总数据，统计结果

会议名称	域名系统相关论文数量
IEEE Security & Privacy	23
ACM CCS	35
USENIX Security	41
ISOC NDSS	45
ACM IMC	109

安全会议论文检索系统 https://secpaper.cn

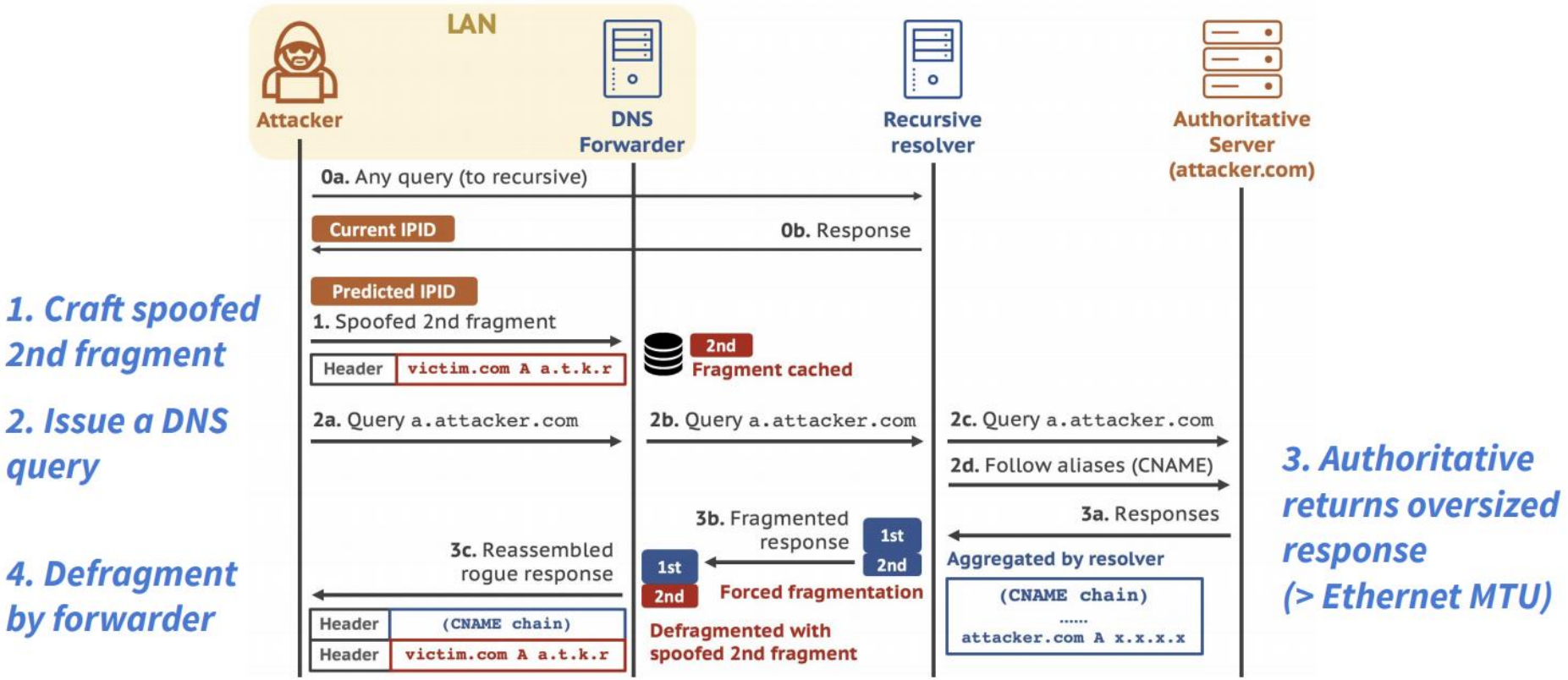
实验室团队关于域名系统的研究成果

- 域名协议安全研究方面
  - 域名系统安全漏洞发现
    - **NDSS 2012: 幽灵域名攻击**
    - **USENIX Security 2018: 域名解析链路劫持**
    - **USENIX Security 2020: DNS转发器缓存污染攻击**
    - **CCS 2020: DNS侧信道缓存污染攻击（Distinguished Paper Award）**

- 域名系统测量研究方面
  - 域名空间及系统新特性测量
    - **DSN 2018: 国际化域名**
    - **IMC 2019: DNS加密协议测量 （IRTF Applied Network Research Prize）**
    - **NDSS 2021: 域名WHOIS系统隐私合规测量**
  - 域名滥用威胁检测
    - **USENIX Security 2016: 泛解析型黑产站群**
    - **CCS 2017: 影子域名**
    - **ACSAC 2019: 在线博彩生态研究**

一、DNS转发器缓存污染攻击

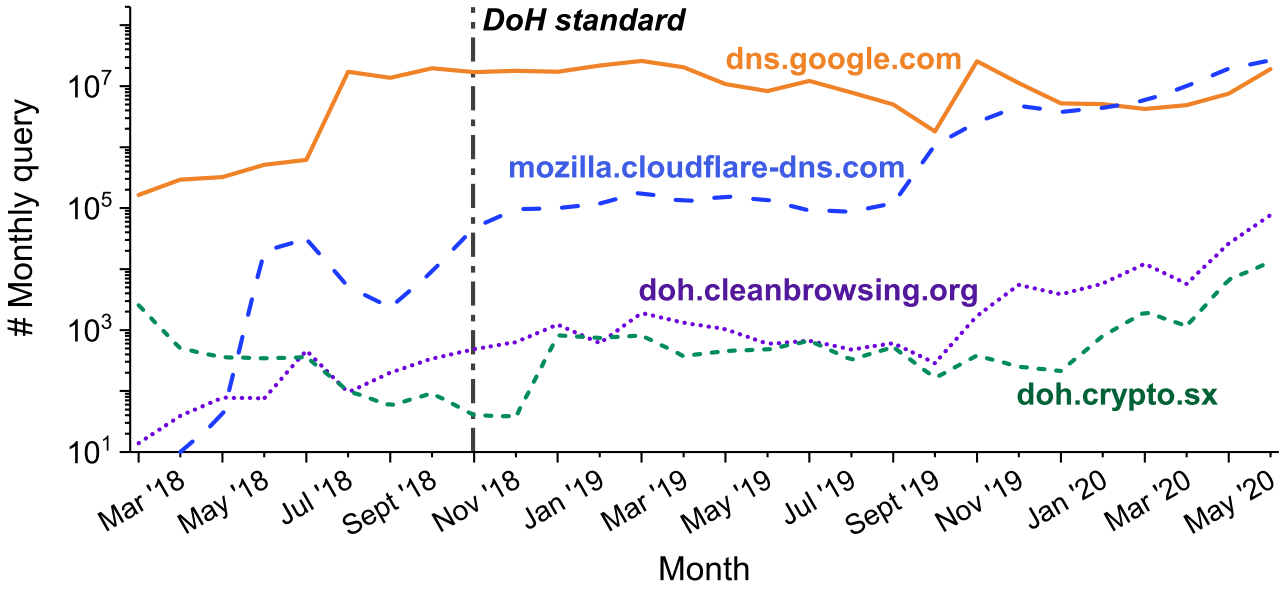
- 研究论文录用于USENIX Security 2020
  - 2款知名DNS软件受影响，8款主流家用路由器受影响



利用DNS分片攻击，污染DNS转发器的缓存记录

二、加密DNS协议测量研究

- 研究论文录用于IMC 2019
  - 大规模测量域名加密协议应用现状，发现部署中的安全隐患
  - 获得 IRTF ANRP 2020 应用网络研究奖




Internet Society

Applied Networking Research Prize
Certificate of Award

Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang and Jianping Wu

for their paper

An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?

Awarded by Internet Research Task Force at the IETF 108 Meeting online in Madrid 25-31 July 2020

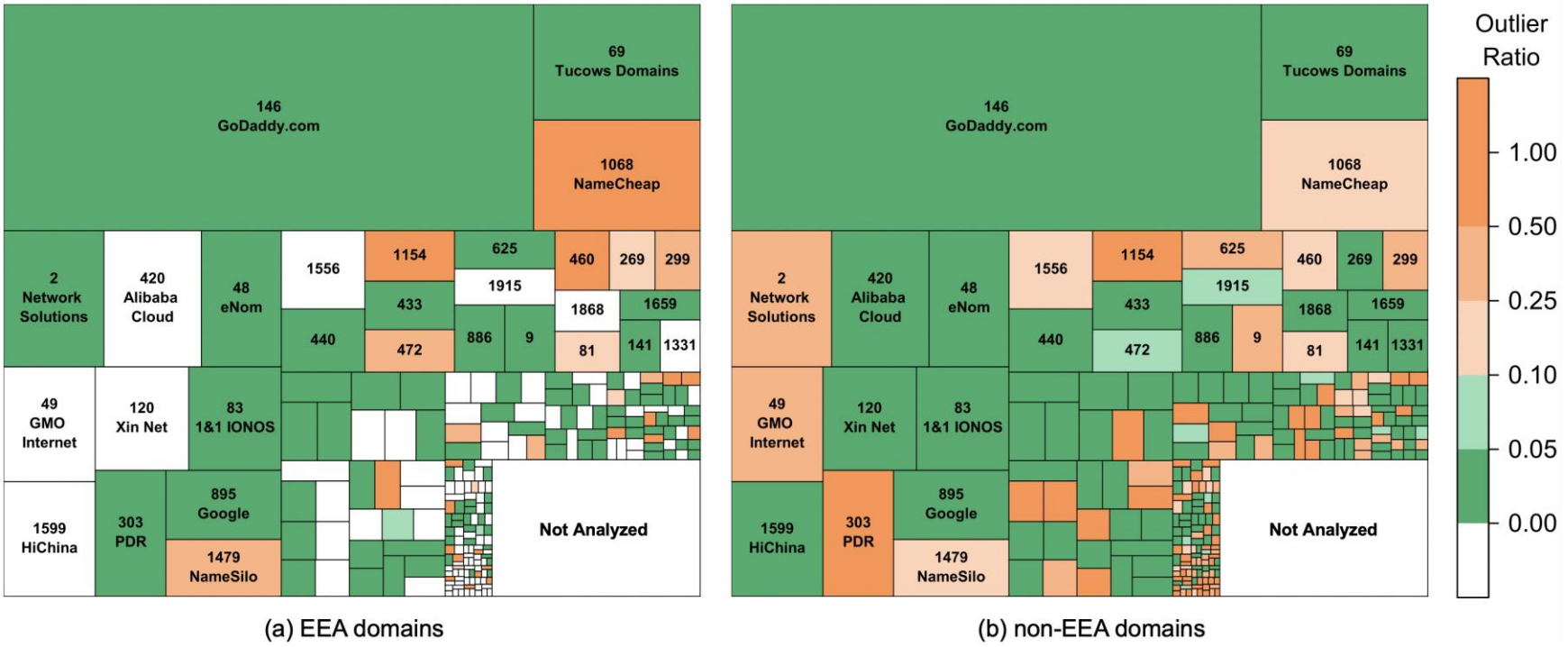
Colin Perkins, IRTF Chair

Matthew D. Ford, Internet Society

加密DNS的网络流量，呈现显著上升趋势

三、域名WHOIS系统隐私合规问题研究

- 研究论文录用于NDSS 2021
  - 量化评估欧盟GDPR隐私保护法规对域名WHOIS系统的影响



欧盟GDPR法规对域名WHOIS系统的实际影响，远超预期

如何结合域名安全学术研究能力，服务于 CERNET 群体？

计划提纲

一、教育网公益域名解析系统

二、校园网DNS威胁情报分析系统

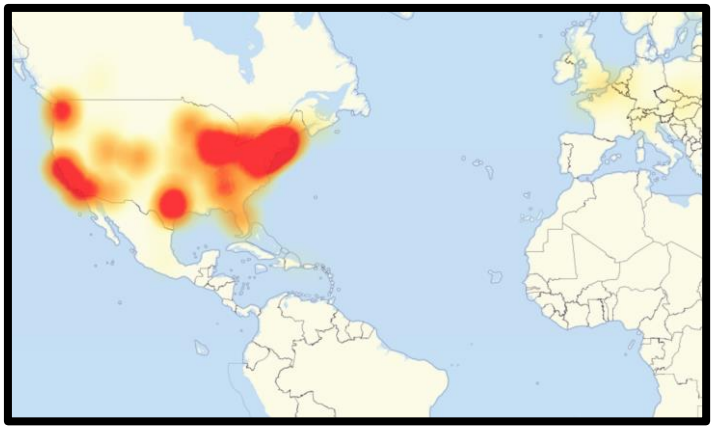
计划一：教育网公益域名解析系统

教育网公益域名解析系统

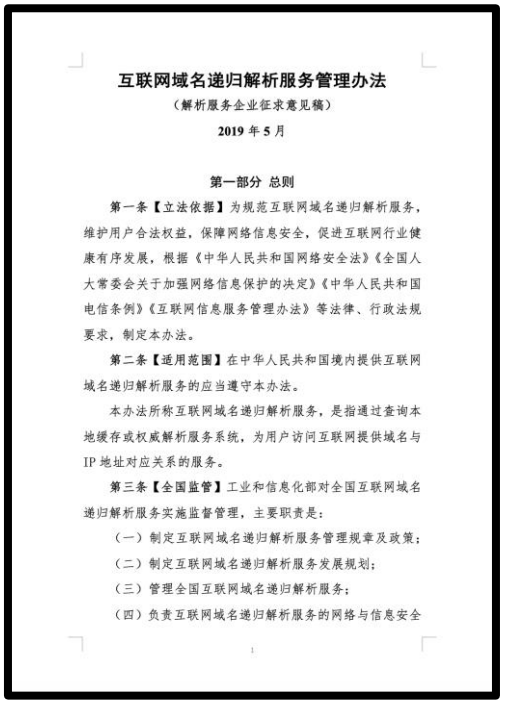
需求及现状分析

域名系统对互联网的基础地位得到广泛重视

- 域名解析服务的正常运行，对互联网安全稳定至关重要
- 国内政府部门逐渐加强对递归域名解析服务的监管举措



2016年，北美大面积断网



互联网域名递归解析服务管理办法

（解析服务企业征求意见稿）

2019 年 5 月

第一部分 总则

第一条【立法依据】为规范互联网域名递归解析服务，维护用户合法权益，保障网络信息安全，促进互联网行业健康有序发展，根据《中华人民共和国网络安全法》《全国人大常委会关于加强网络信息保护的决定》《中华人民共和国电信条例》《互联网信息服务管理办法》等法律、行政法规要求，制定本办法。

第二条【适用范围】在中华人民共和国境内提供互联网域名递归解析服务的应当遵守本办法。

本办法所称互联网域名递归解析服务，是指通过查询本地缓存或权威解析服务系统，为用户访问互联网提供域名与IP地址对应关系的服务。

第三条【全国监管】工业和信息化部对全国互联网域名递归解析服务实施监督管理，主要职责是：

（一）制定互联网域名递归解析服务管理规章及政策；

（二）制定互联网域名递归解析服务发展规划；

（三）管理全国互联网域名递归解析服务；

（四）负责互联网域名递归解析服务的网络与信息安全

递归解析服务管理办法

高校自建的域名解析服务易存在安全隐患

- 安全方面：配置管理不当十分常见，安全增强协议部署缓慢
- 性能方面：对域名解析优化不足，直接影响网络访问性能

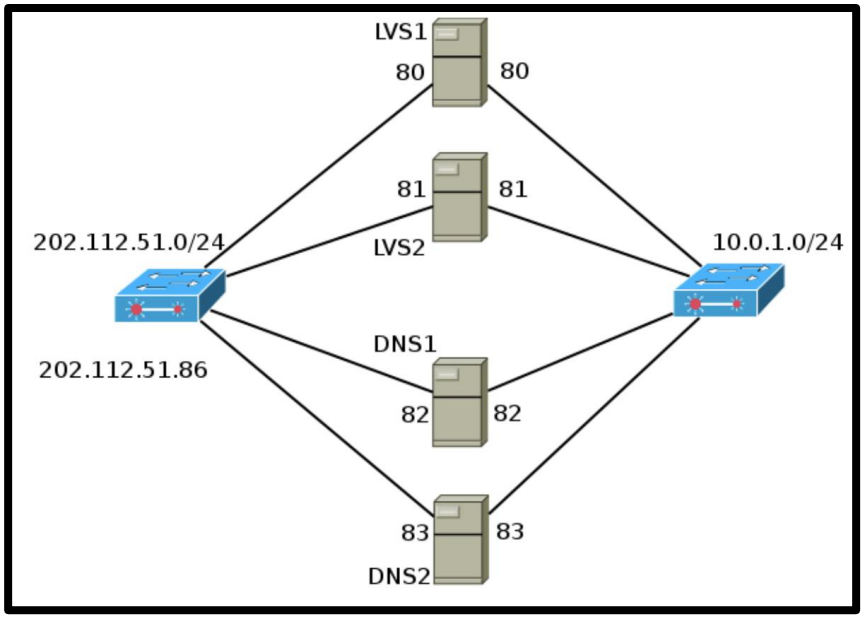
配置管理不当类型	域名数量/规模
匿名区域传输	36
NSEC记录子域名枚举	23
匿名区域文件更新	4
NS记录配置不当	1248
开放递归解析服务器	> 8千

教育系统所属高校，仅有58个域名部署DNSSEC协议

参阅：《2020年互联网基础设施安全白皮书》

CERNET现有公共域名解析服务，规模较小

- CERNET现有公共域名递归解析服务建设于2013年，系统架构有待改进 （地址：101.7.8.9）
- 长期以来，CERNET公共域名递归解析服务，用户规模较小，影响力有限，难以支撑高水平研究工作



域名系统负载均衡网络拓扑图

无法满足高校群体绿色上网，科学上网需求

- 绿色上网：对赌博，色情等恶意域名进行访问阻断
- 科学上网：面向高校可信用户，提供科学上网渠道

某高校校园网边界，赌博色情类域名检测结果

教育网公益域名解析系统

建设方案

升级完善教育网现有递归解析服务

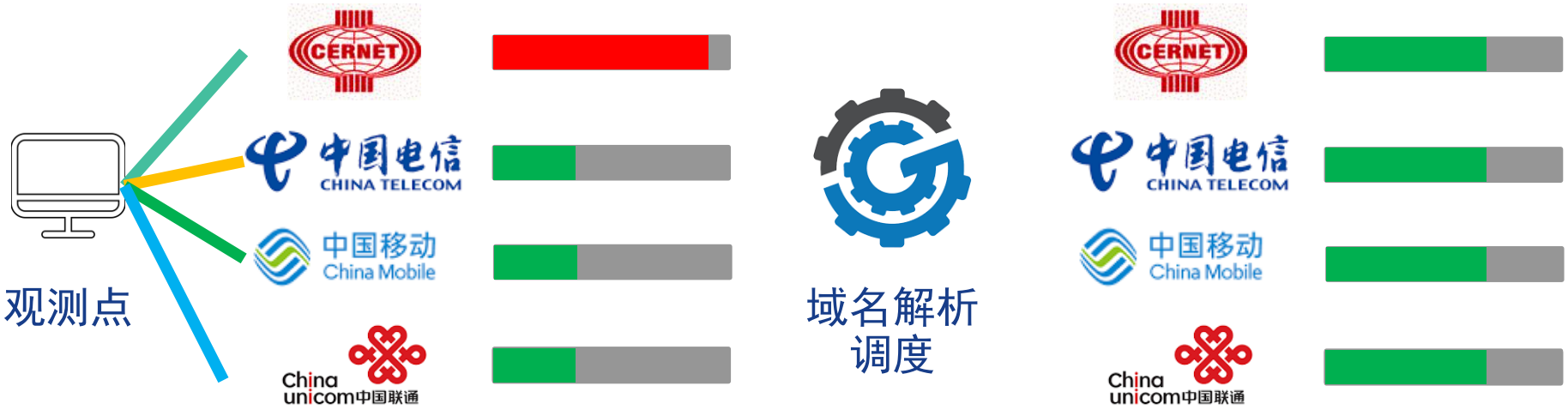
- 传统域名解析服务 主服务器
  - 主机地址：101.7.8.9
  - Anycast节点：北京，上海，广州，武汉，成都
  - 沿用现有主机地址，面向教育网用户群体提供服务
  - 采用114公共DNS解决方案，对软件服务进行升级

- 加密域名解析服务 备服务器
  - 主机地址：101.7.7.7
  - 同时提供DNS-over-TLS及DNS-over-HTTPS加密域名解析服务
  - 结合大型安全厂商威胁情报知识，提供绿色上网服务

面向多出口环境，提供智能域名解析调度

- 背景：对域名解析优化不足，易影响网络访问延迟

- 基于已有学术成果，提供智能域名解析调度的解决方案
  - 寻找最优解析结果：Science China，Finding the Best Answer
  - 抵抗缓存污染攻击：SATIN 12，DNS Hold on



自动调整DNS各线路解析比例

教育网公益域名解析系统

预期目标及成效

预期建设目标及成效

- 为教育网用户提供稳定的域名解析服务
  - 预计能够支持数百高校，最大支持一千万QPS的查询请求服务
  - 提供 7*24 小时应急响应服务
  - 为欠缺DNS建设能力的高校，提供统一的域名解析与托管服务
- 为政府部门安全监管提供一定支持
  - 阻断恶意域名访问
  - 实现对特定域名一键断网
- 为增强教育网公益域名解析系统的影响力
  - 相关数据可用于支撑高水平学术研究
  - 域名系统可纳入互联网关键基础设施，作为HW行动攻击目标

计划二：校园网DNS威胁情报分析系统

校园网DNS威胁情报分析系统

需求及现状分析

教育系统所属高校经常成为网络攻击的目标

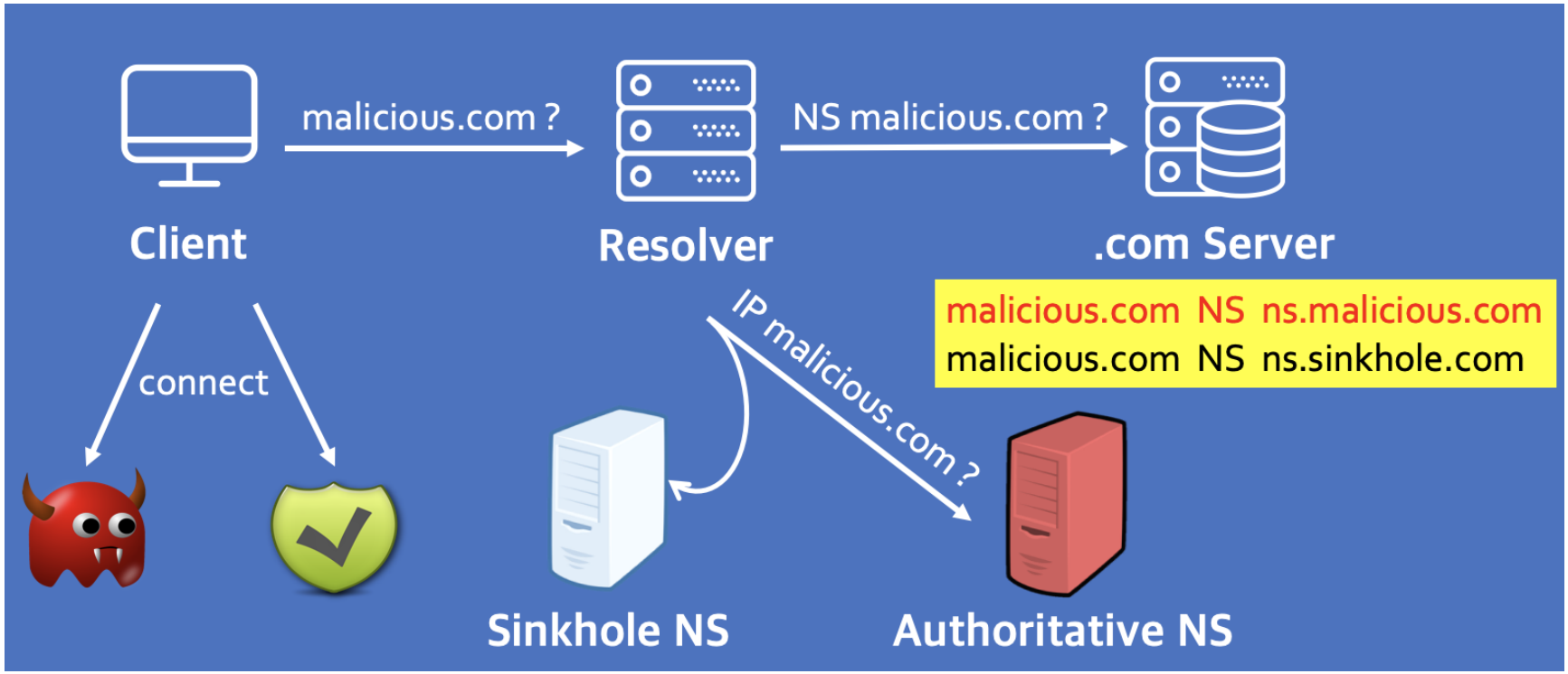
- 教育系统域名及站点，在搜索引擎中具有高权重

教育系统所属高校经常成为网络攻击的目标

- 相比与知名企业，普通高校的安全防御能力相对较为薄弱

基于域名系统，发现并阻断安全风险

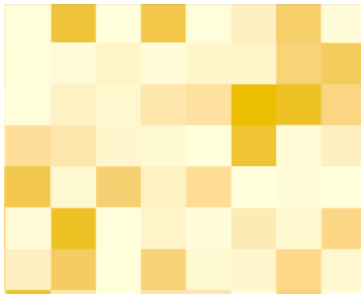
- 核心优势一：结构极其简单 → 部署特别方便



基于域名系统，发现并阻断安全风险

- 核心优势一：结构极其简单 → 部署特别方便
- 核心优势二：应用极其广泛 → 防御特别广谱

恶意软件



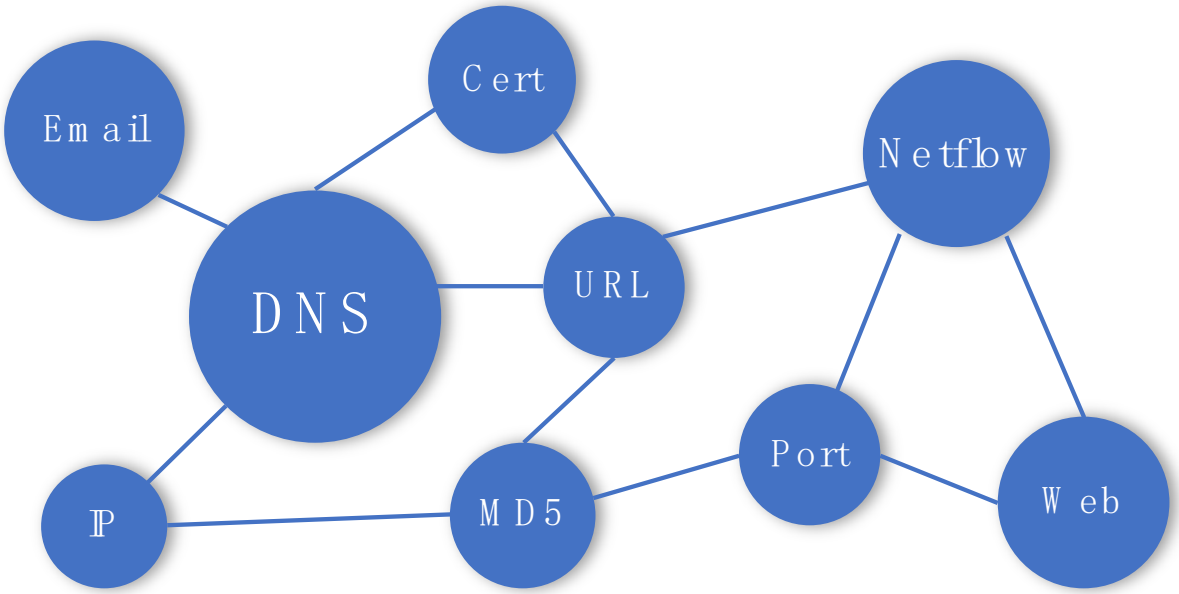
色情赌博

隐蔽通信

域名解析同样也是恶意网络活动的起点

DNS + 威胁情报具有的巨大优势

- 一个目标：安全防御
- 两个手段：威胁情报 + 域名访问拦截
- 主要优势：用户接入方便，防御能力广谱



看得全
发现早
挖的深
串得广

Visibility: Security insights from big data

DNS数据安全分析的显著挑战

- 主流趋势：大规模自动化地威胁发现与处理
- 实际痛点与挑战
  - 拥有数据的门槛
  - 处理数据的门槛
  - 解读数据的门槛

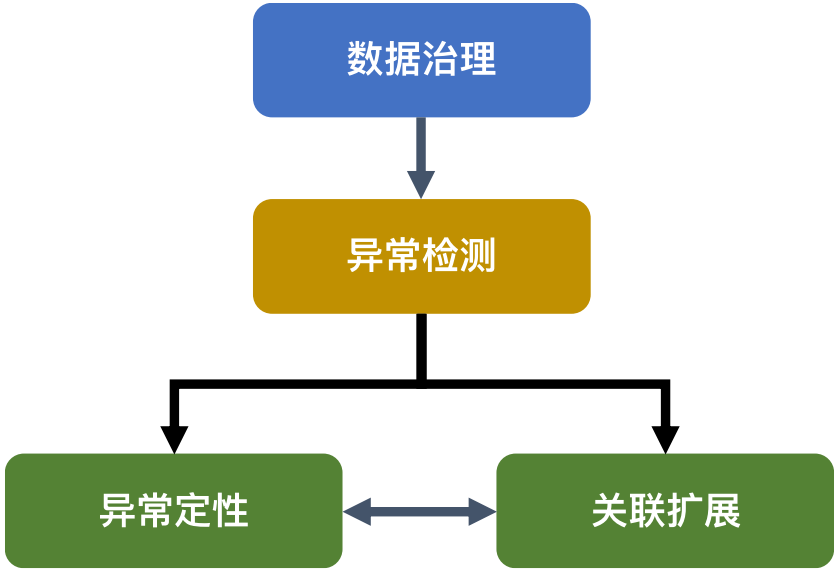
恶意样本库

沙箱日志库

网址数据库

域名信息库

安全大数据

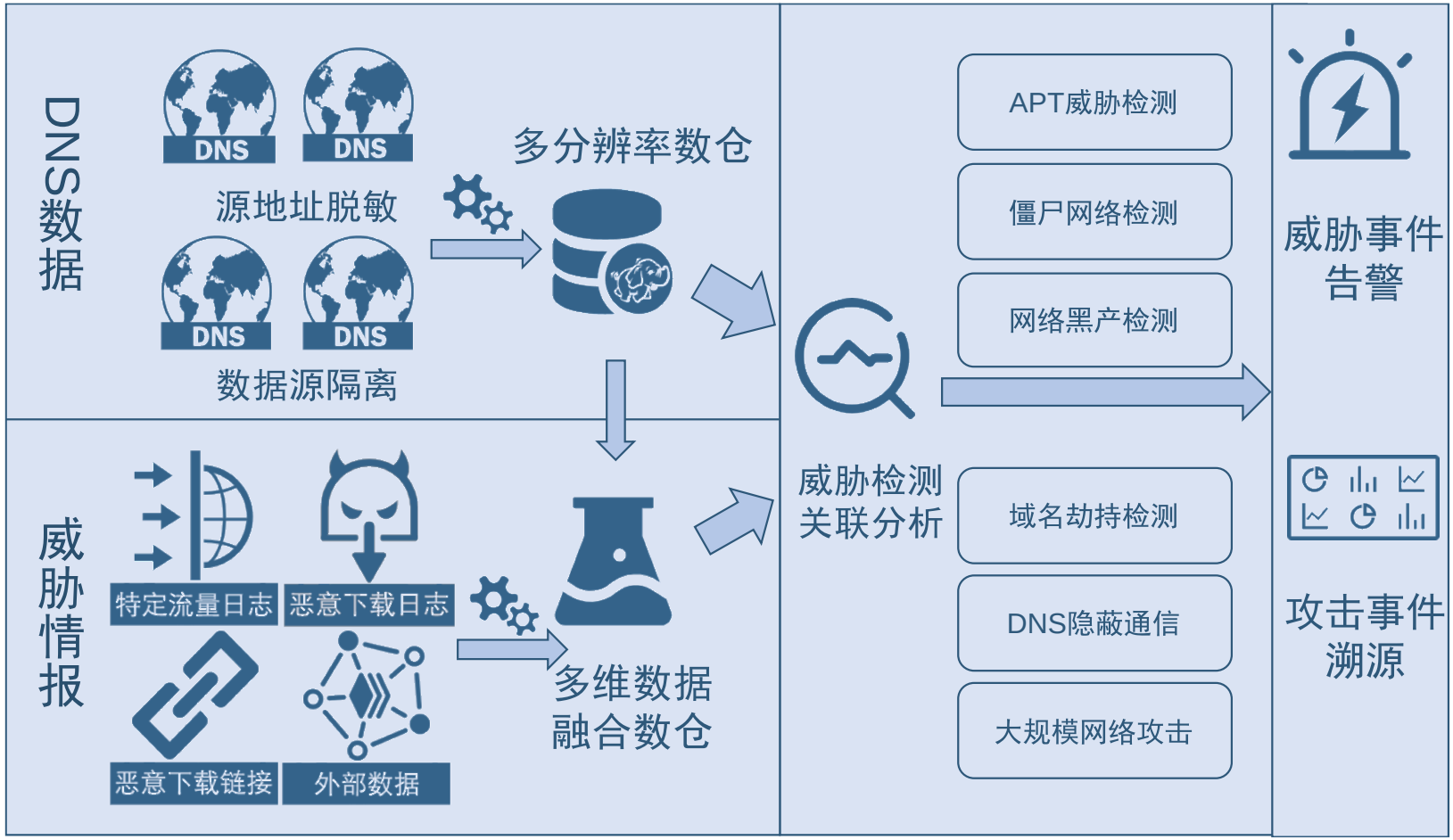


DNS数据安全分析主要结构

校园网DNS威胁情报分析系统建设方案

校园网DNS威胁情报分析系统架构图

- 核心思路：结合安全厂商海量威胁情报数据，面向教育系统所属高校，提供集中地、统一地校园网DNS日志威胁情报分析服务

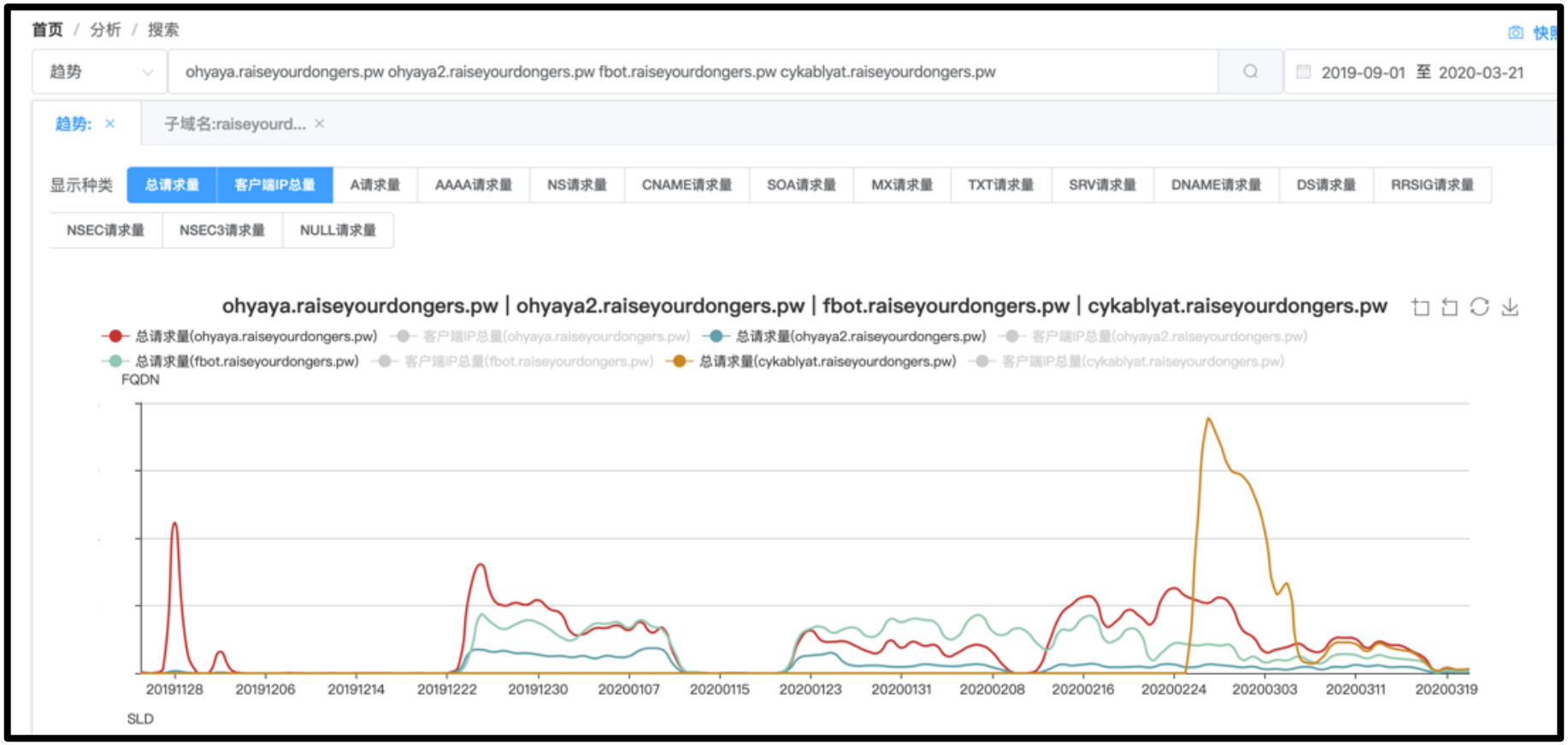


校园网DNS威胁情报分析系统

现有成果

域名解析异常趋势变化分析

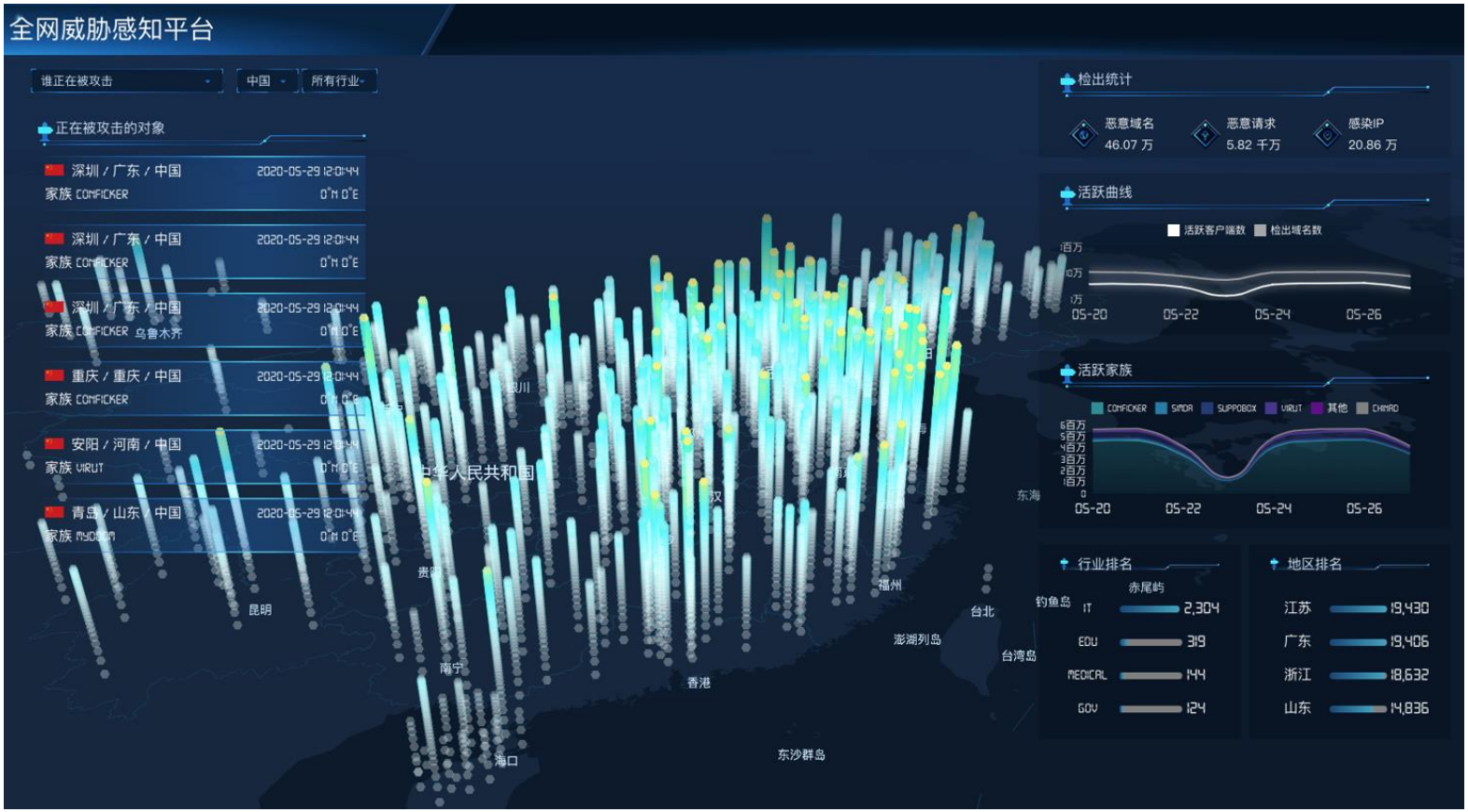
- 及时追踪域名解析中异常趋势



域名访问激增；域名关联共生

僵尸网络家族活跃态势

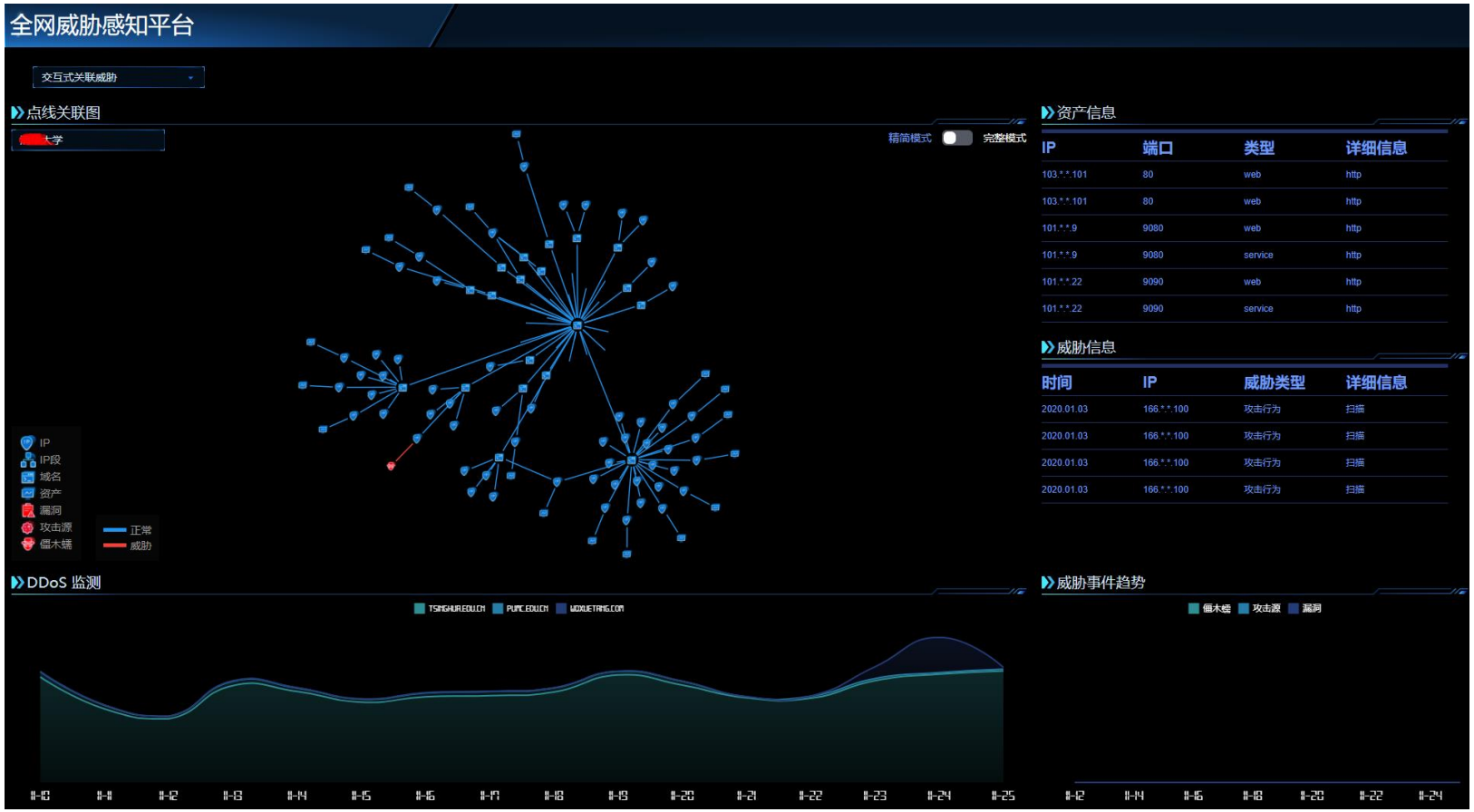
- 实时呈现正在被攻击的受害主机



活跃家族信息分析

图系统在安全威胁关联扩展中的应用

- 深度数据融合，简易呈现数据资产关联关系



IP，IP段，域名，漏洞，端口，攻击源

计划提纲

一、教育网公益域名解析系统

二、校园网DNS威胁情报分析系统

清华大学 Tsinghua University

2020年CERNET学术年会
网络安全论坛

CERNET DNS安全服务与威胁情报分析

刘保君

清华大学网络研究院

lbj@mail.tsinghua.edu.cn