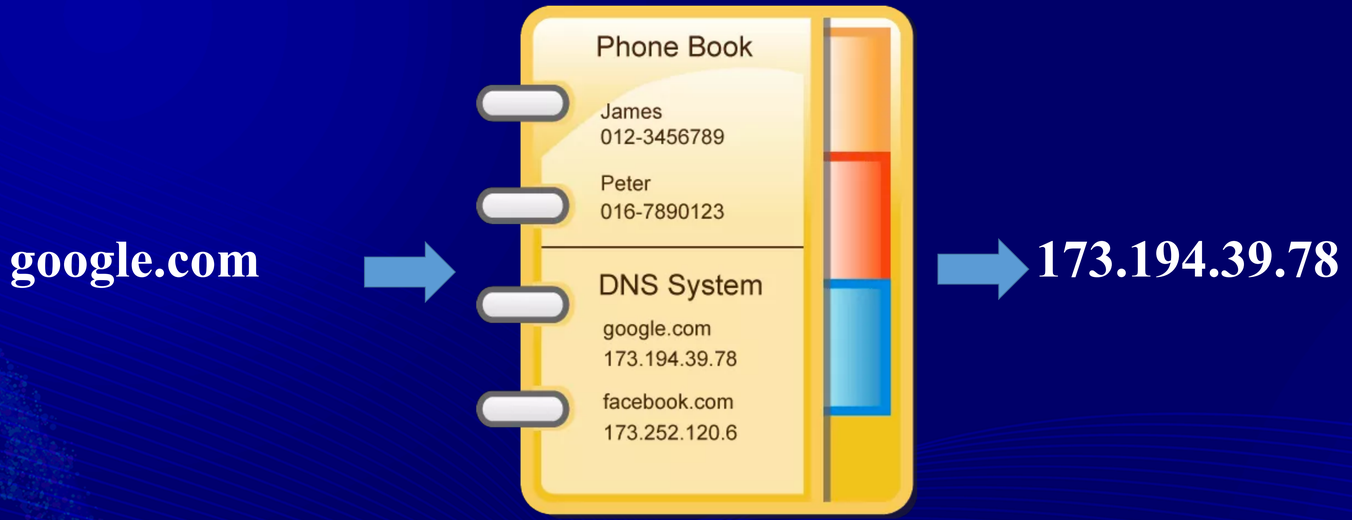
# 域名空间治理与域名协议安全的演进

段海新，教授
清华大学-奇安信联合研究中心

- 为什么关注DNS安全？
- 根域名的历史和域名空间扩展
- DNS协议攻击和协议安全的演进

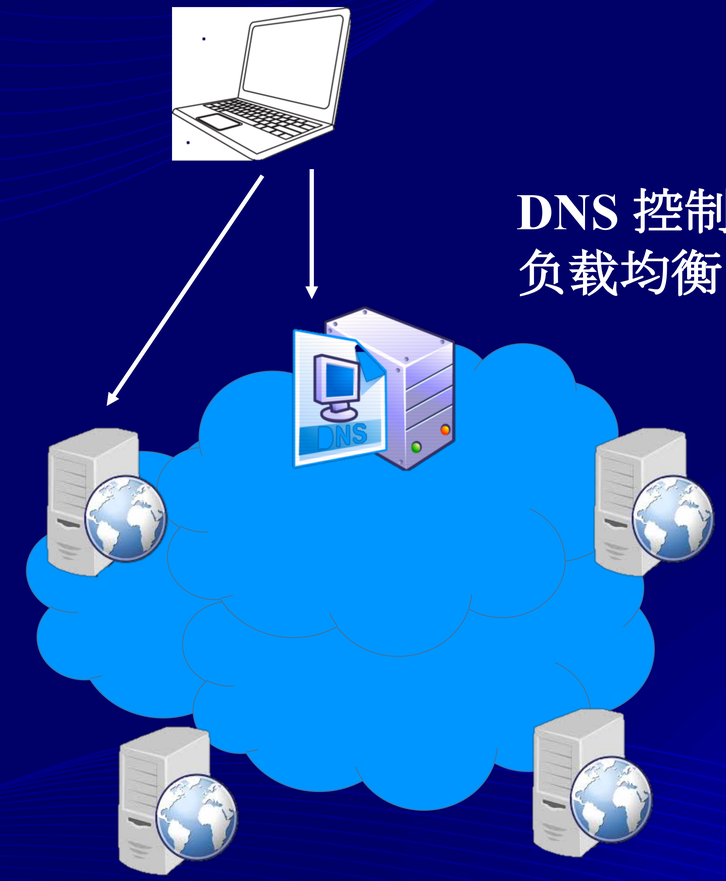
# DNS 是互联网重要的基础服务

- DNS 是互联网重要的基础服务
- <域名,IP地址>映射的数据库



# CDN基于DNS提供内容分发和负载均衡

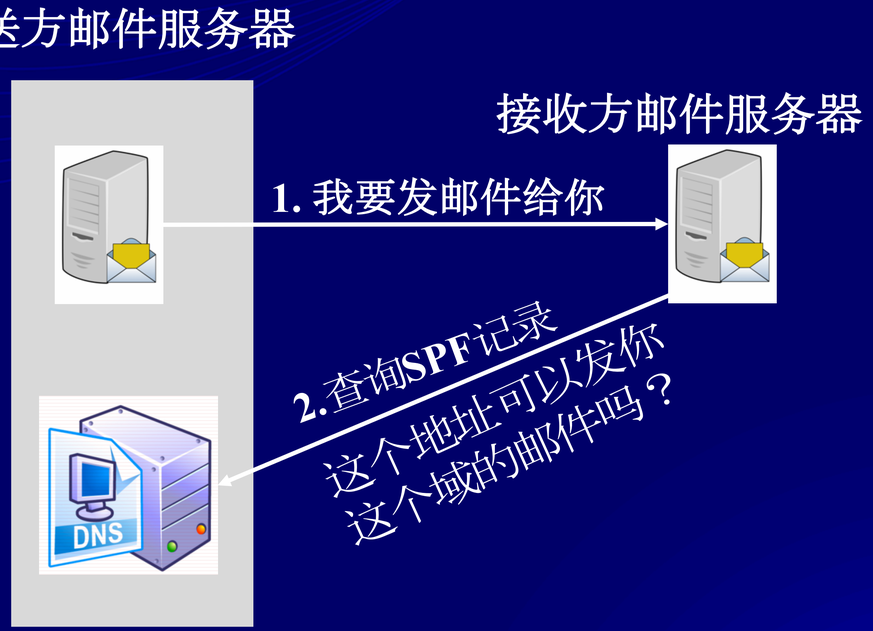
- DNS 是互联网重要的基础服务
- <域名,IP地址>映射的数据库
- 应用层的路由
  - CDN基于DNS提供内容分发、负载均衡




DNS 控制内容路由、
负载均衡

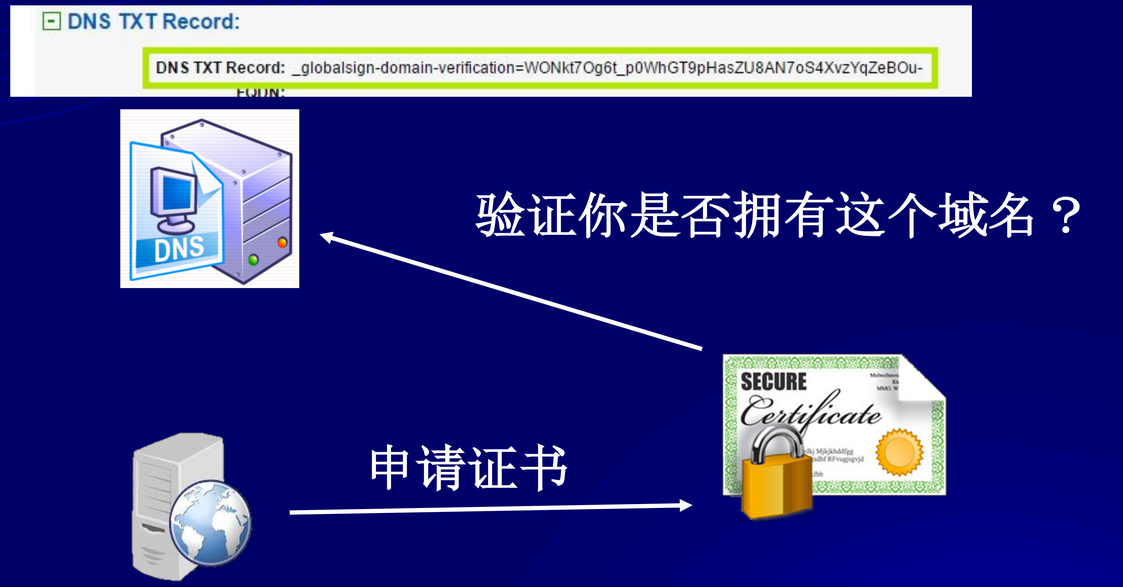
# DNS作为信任的基础支持邮件服务器的验证

- DNS 是互联网重要的基础服务
- <域名,IP地址>映射的数据库
- 应用层的路由
  - CDN基于DNS提供内容分发、负载均衡
  - 电子邮件的路由 (MX)
- DNS 作为信任的基础
  - 邮件服务器验证（SPF）,防垃圾邮件



# DNS作为信任的基础支持公钥证书申请

- DNS 是互联网重要的基础服务
- <域名,IP地址>映射的数据库
- 应用层的路由
  - CDN基于DNS提供内容分发、负载均衡
  - 电子邮件的路由 (MX)
- DNS 作为信任的基础
  - 邮件服务器验证（SPF），防垃圾邮件
  - 公钥证书申请中的验证



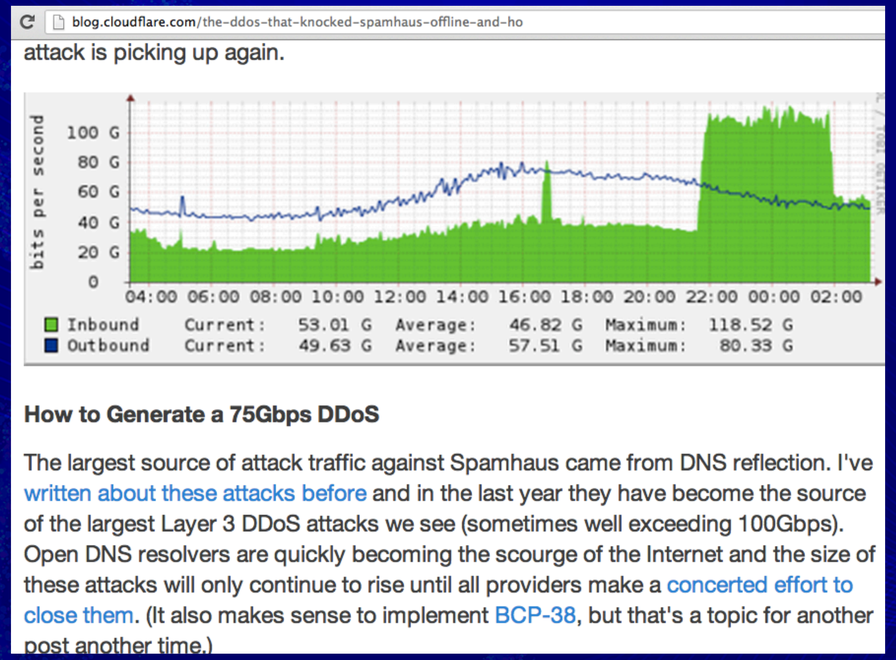
# DNS作为公钥基础设施（PKI）

- DNS 是互联网重要的基础服务
- <域名,IP地址>映射的数据库
- 应用层的路由
  - CDN基于DNS提供内容分发、负载均衡
  - 电子邮件的路由 (MX)
- DNS 作为信任的基础
  - 邮件服务器验证（SPF）,防垃圾邮件
  - 公钥证书申请中的验证
- DNS 作为公钥基础设施PKI
  - DNSSEC：DS, RRSIGN,DNSSKEY…
  - TLSA：关联Web服务器的TLS证书（RFC 6698,2012）

# DNS相关的攻击常导致互联网大规模瘫痪

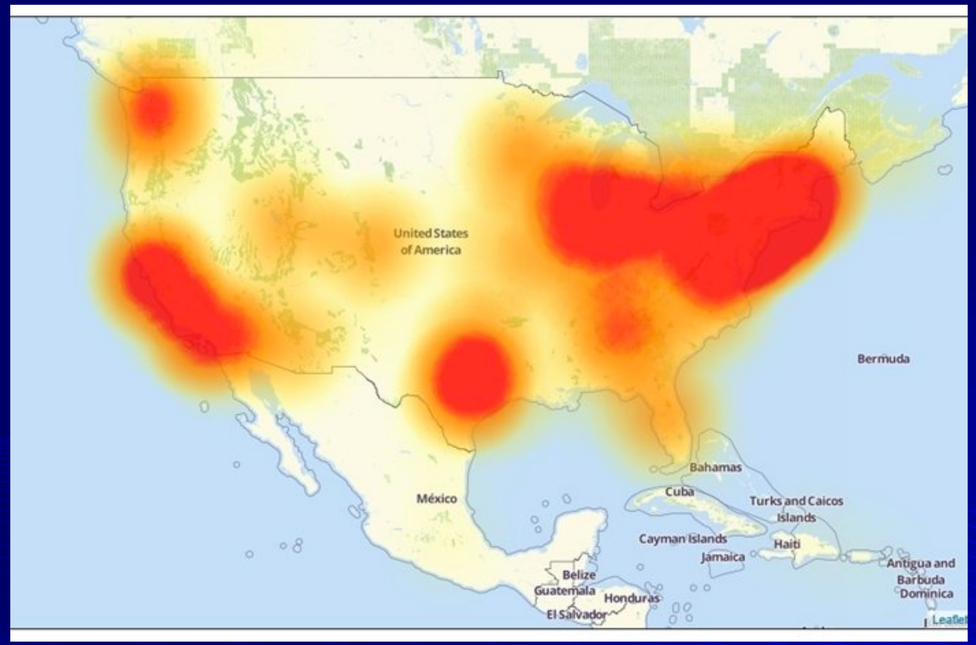
- **DNS作为DDoS攻击工具**

Spamhause DNS reflection，2013



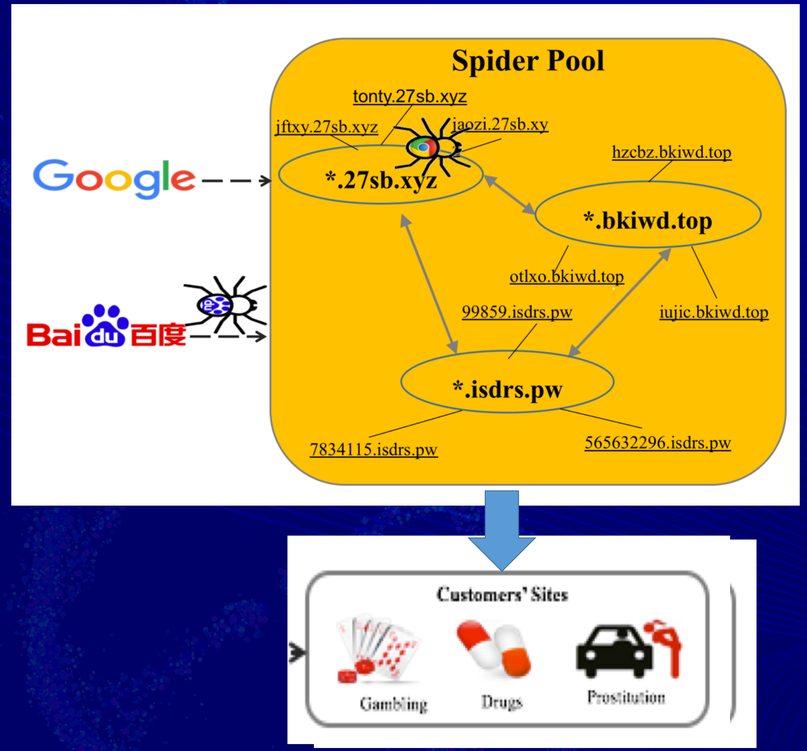

- **DNS 作为攻击目标**

Dyn 攻击事件， 2016

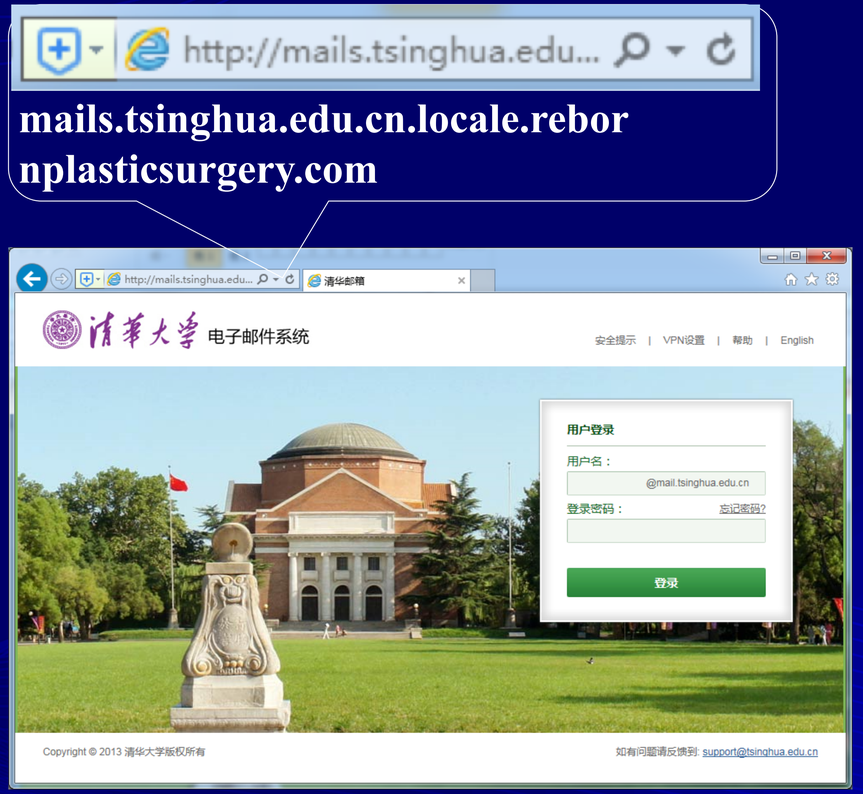


# 域名的滥用：地下黑产和网络犯罪

- 利用域名搭建蜘蛛池，实现搜索引擎污染，推广赌博、毒品等违法网




- 伪装成合法域名进行钓鱼攻击



# DNS是互联网治理的焦点

- DNS是互联网治理的焦点，涉及技术标准、国际政治、法律经济等各种纠纷

关于伊拉克国家域名IQ被删除的事件：

伊拉克战争期间，在美国政府授意下，伊拉克顶级域名“.iq”的申请和解析工作被终止，所有网址以“.iq”为后缀的网站从互联网蒸发

关于IPv6试验根项目：

中国部署了4台IPv6根域名服务器。打破垄断、突破封锁，中国彻底打破了没有根服务器的困境。

- 为什么关注DNS安全？
- 根域名的历史和域名空间扩展
- DNS协议攻击和协议安全的演进

# DNS早期的历史

- 1970s， APARNET创立之初， SRI-NIC负责维护HOSTS.TXT
- 1980+， Jon Postel & Paul Mockapetris DNS协议和软件， 运行第一个Root Server
- 1985年4个根域名服务器, 1990年扩展到7个

| Name | IP Address | Software | Organization |
|---|---|---|---|
| SRI-NIC | 10.0.0.51<br>26.0.0.73 | JEEVES | SRI International |
| ISIB[10] | 10.3.0.52 | JEEVES | Information Sciences Institute, USC |
| ISIC | 10.0.0.52 | JEEVES | Information Sciences Institute, USC |
| BRL-AOS | 192.5.25.82<br>128.20.1.2 | BIND | Ballistic Research Laboratory, U.S. Army |

1985年， 4个root server

| Original Name | New Name | IP Address | Organization |
|---|---|---|---|
| SRI-NIC.ARPA | NS.NIC.DDN.MIL | 192.67.67.53 | SRI International |
| A.ISI.EDU | A.ISI.EDU | 26.2.0.103<br>128.9.0.107 | Information Sciences Institute, USC |
| C.NYSER.NET | C.NYSER.NET | 192.33.4.12 | RPI |
| TERP.UMD.EDU | TERP.UMD.EDU | 128.8.10.90 | University of Maryland |
| GUNTER-ADAM.ARPA | GUNTER-ADAM.AF.MIL | 26.1.0.13 | U.S. Air Force Networking Group |
| NS.NASA.GOV | NS.NASA.GOV | 128.102.16.10<br>192.52.195.10 | NASA Ames Research Center |
| BRL-AOS.ARPA | AOS.BRL.MIL | 192.5.25.82<br>128.20.1.2 | Ballistic Research Laboratory, U.S. Army |

1990年， 7个root server

# 1990s：DNS随互联网扩大和商业化迅速发展

- 域名注册转到NSI公司（后被VeriSign收购），引发域名的战争
- 互联网在全球迅速发展，欧洲、日本部署了两个根
- 继续扩展受 DNS 消息大小限制（<512字节），无法部署更多
- 1995年，改名[a-i].root-servers.net，压缩后可支持13个根

| Name | IP Address | Organization |
|---|---|---|
| NS.NIC.DDN.MIL | 192.112.36.4 | Network Solutions, Inc. |
| KAVA.NISC.SRI.COM | 192.33.33.24 | SRI International |
| C.NYSER.NET | 192.33.4.12 | NYSERnet |
| TERP.UMD.EDU | 128.8.10.90 | University of Maryland |
| NS.NASA.GOV | 128.102.16.10<br>192.52.195.10 | NASA Ames Research Center |
| NIC.NORDU.NET | 192.36.148.17 | NORDUnet |
| AOS.BRL.MIL | 192.5.25.82 | Ballistic Research Laboratory, U.S. Army |

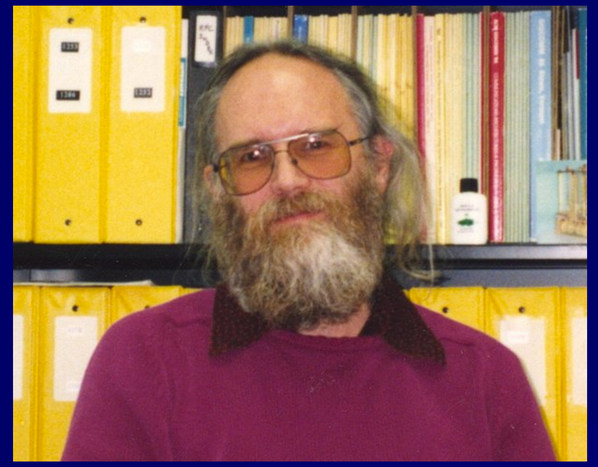
Root Servers, 1991

| Original Name | New Name | Organization |
|---|---|---|
| NS.INTERNIC.NET | A.ROOT-SERVERS.NET | InterNIC (operated by NSI) |
| NS1.ISI.EDU | B.ROOT-SERVERS.NET | Information Sciences Institute, USC |
| C.PSI.NET | C.ROOT-SERVERS.NET | PSINet |
| TERP.UMD.EDU | D.ROOT-SERVERS.NET | University of Maryland |
| NS.NASA.GOV | E.ROOT-SERVERS.NET | NASA Ames Research Center |
| NS.ISC.ORG | F.ROOT-SERVERS.NET | Internet Software Consortium |
| NS.NIC.DDN.MIL | G.ROOT-SERVERS.NET | GSI (operated by NSI) |
| AOS.ARL.ARMY.MIL | H.ROOT-SERVERS.NET | U.S. Army Research Lab |
| NIC.NORDU.NET | I.ROOT-SERVERS.NET | NORDUnet |

Renaming of Root Servers, 1995

# Jon Postel: 互联网之神





- Jon Postel领导的IANA 负责Root DNS管理
- 选择Root server托管组织的原则[2]
  - 需要：对根服务器有需求
  - 连通：内部和外部都有广泛的连接
  - 共识：来自社区内部的广泛支持
  - 不做过滤：承诺对于发出和收到的流量都不做过滤
- 国家域名（ccTLD）的分配
  - 主要考虑：有技术能力、可信、公正（RFC 1591，1994）
  - 例：IQ在1997分配给美国公司，负责人2002年被捕，2005由ICANN重新分配给伊拉克通信管理局[1]

[1]https://www.iana.org/reports/2005/iq-report-05aug2005.pdf
[2] https://www.icann.org/en/system/files/files/rssac-023-04nov16-en.pdf

# 关于域名的战争和互联网治理早期的历史




- 在互联网成立之初，美国政府对互联网DNS根的控制几乎是不存在的
- 大多数政策问题上，政府相信技术社区
- 在域名管理问题上，技术社区相信Jon Postel

从根上治理互联网：互联网治理与网络空间的驯化

[美] Milton L. Mueller著，段海新 胡泳 译

**Throughout its entire history, the Internet system has employed a central Internet Assigned Numbers Authority (IANA)…**

**----V. Cerf, RFC 1174**

# 1998年ICANN之后的根域名管理

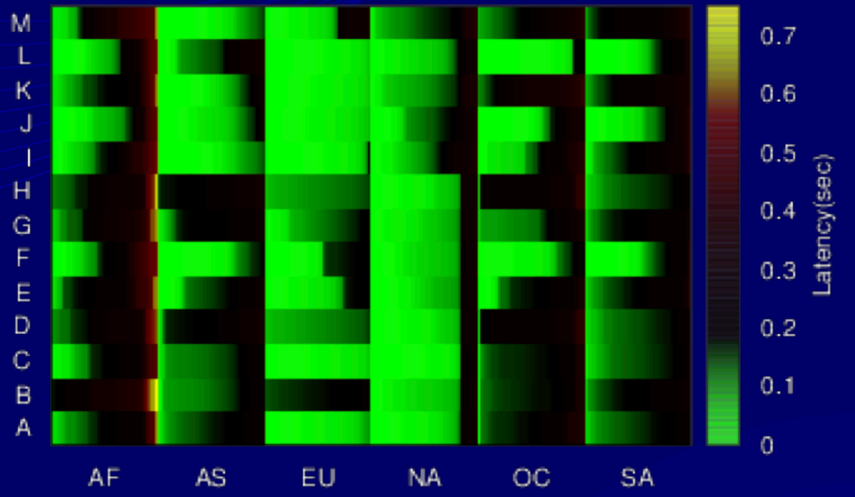
- ICANN/IANA仍是根区数据的权威
  - VeriSign只负责根区文件分发
  - DNSSEC 签名保证根区数据完整性
- 2013年 斯诺登事件爆发
- 2013年 ICANN等组织蒙得维的亚声明[2]
  - 针对美国大规模网络监控的忧虑
  - 强调全球一致，反对国家层面上的互联网分裂
  - 加快ICANN/IANA的国际化
- 2016年IANA监管权移交后，根区文件修改不再需要美国政府批准

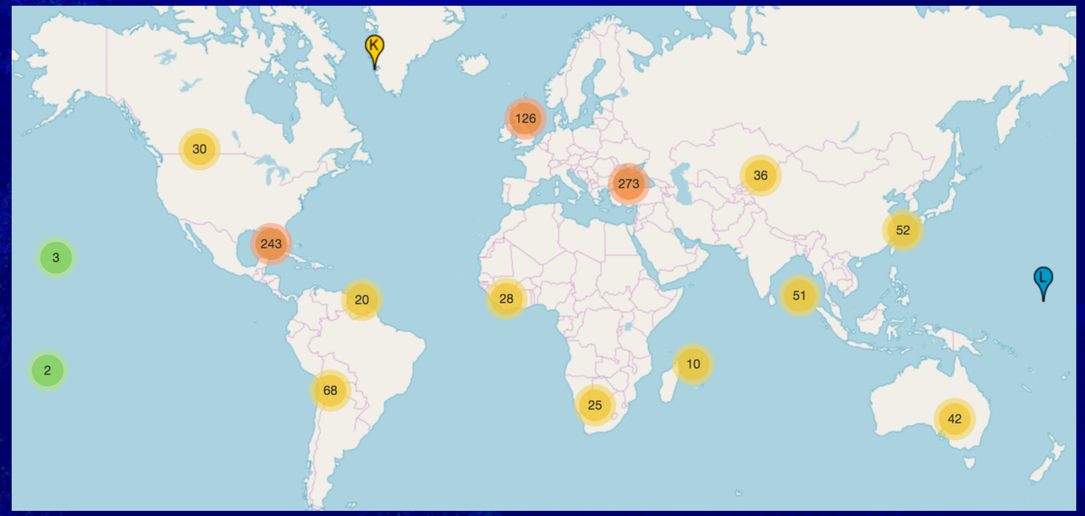
[1] http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm.
[2] https://www.icann.org/news/announcement-2013-10-07-zh

# 根域名服务器的扩展

- Anycast Instance(RFC 3258, 2002)
- 2013年346个，全球延迟不均衡
- 2019/08/15：全球1011个镜像
- 中国大陆已部署至少8个
- 本地根区镜像（RFC 7706，2015）

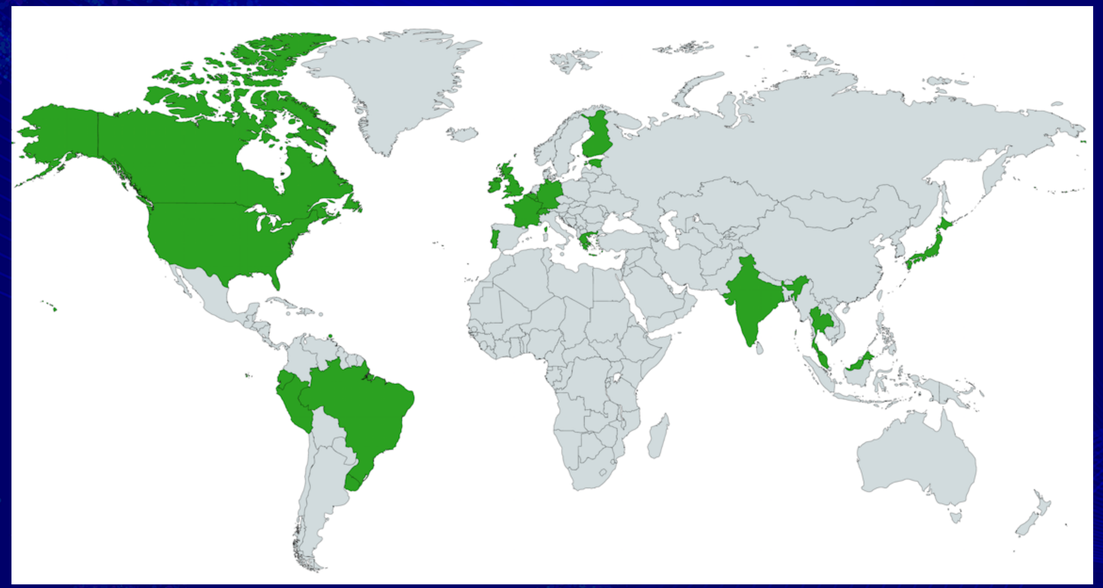
全球各大洲到13个根域名服务器的解析延迟



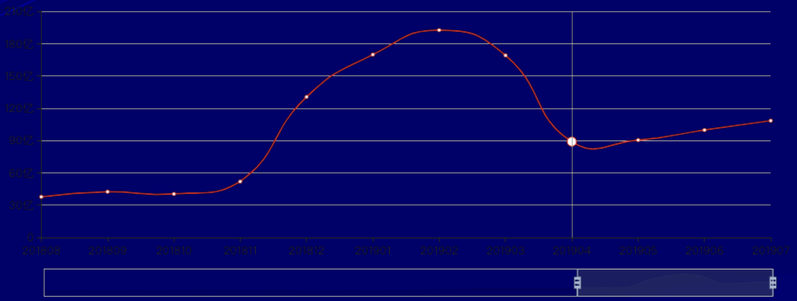

# IPv6网络中的Root 和 AAAA记录

- 2008至今， 所有Root Server都是IPv4/IPv6双栈
- 2018年， ～98%的TLD有IPv6
- Google 统计：24个国家IPv6流量超过15%



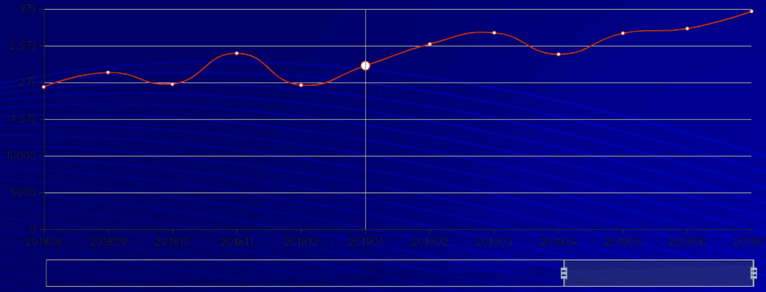
## 客户端的数量大量增长

奇安信 PDNS 统计：中国用户AAAA查询次数



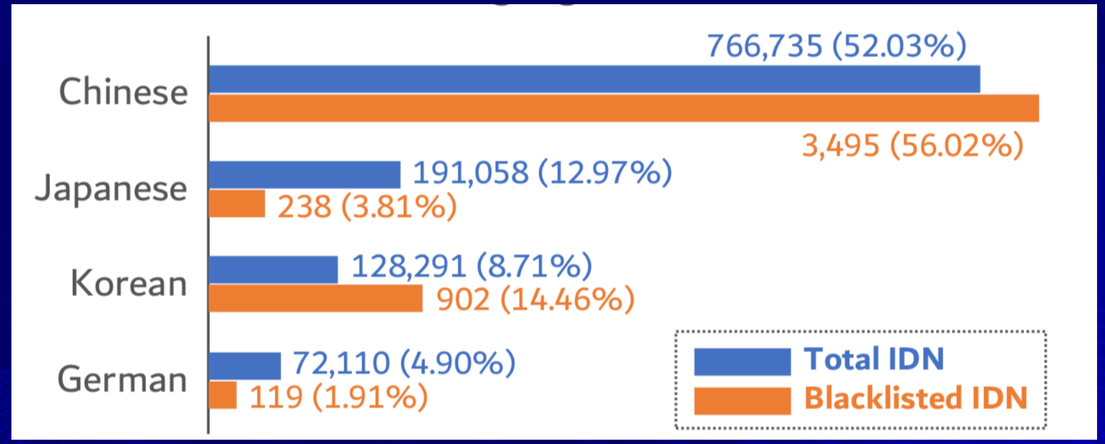
## IPv6的服务器增长相对较慢

奇安信 PDNS 统计：中国访问的IPv6服务器数量



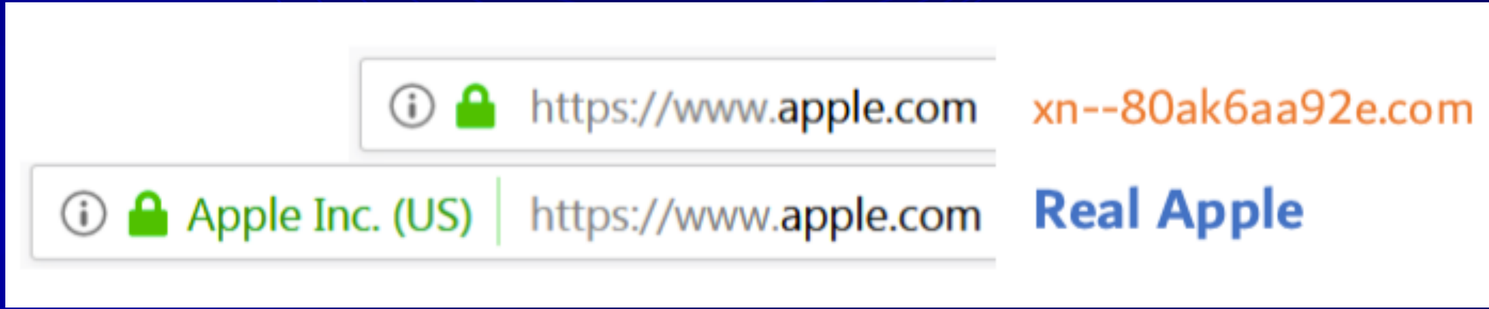
# 名字空间的扩展：国际化域名IDN

- 国际化域名(IDN)
  - 1996年开始研究和讨论
  - 2003年，非ASCII (RFC3490)
  - 2009年 Root 开始iTLD
- 我们关于IDN域名的研究
  - 收集1.5亿域名
    - com, net, org,
    - 53个iTLD
  - 抽取1.4M IDN(~1%)
  - 恶意域名黑名单(VirusTotal等)

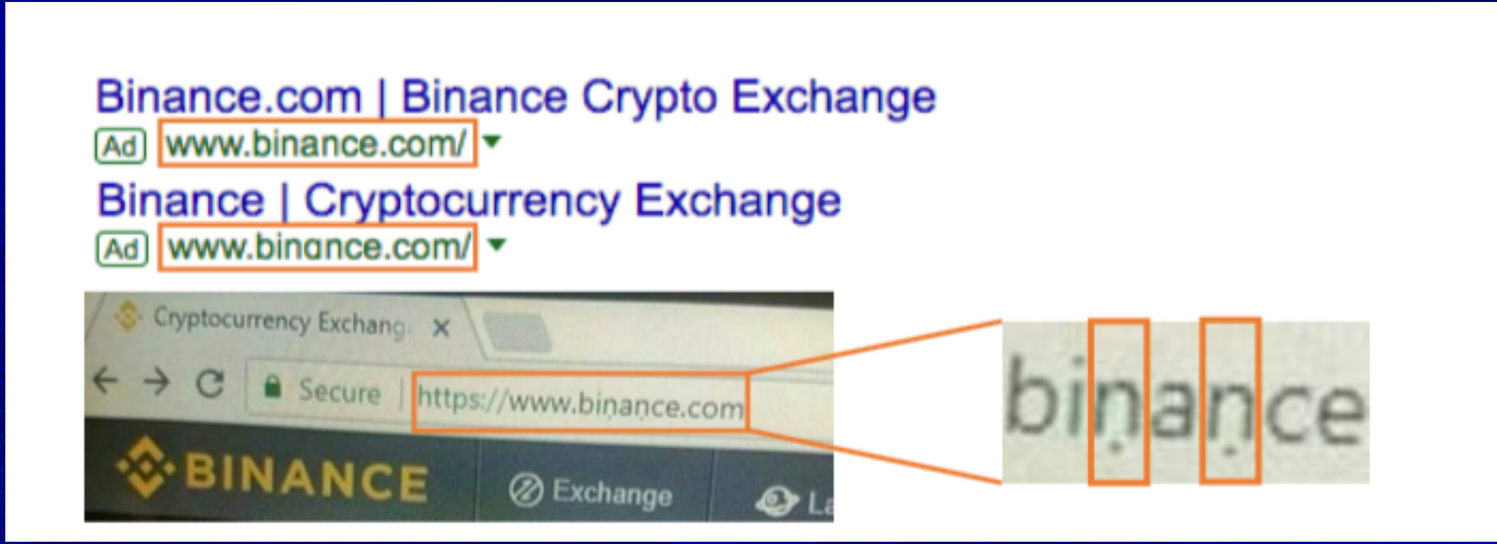



# 同形异义（homographic） IDN域名钓鱼攻击

研究者

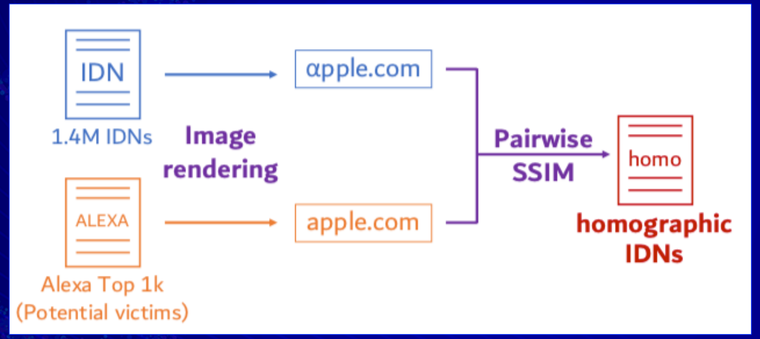



真实的攻击



# 同形异义域名的检测、生成

- 相似度检测同形异义IDN域名




- 像Google.com的IDN域名

| Maximum SSIM Index | IDN | |
|---|---|---|
| | Punycode | Unicode Characters |
| 1.00 | xn--ggle-55da.com | google.com |
| | xn--oole-z7bc.com | google.com |
| 0.99 | xn--googl-r51b.com | google.com |
| | xn--googl-n0a.com | google.com |
| 0.98 | xn--googe-95a.com | google.com |
| | xn--oole-cxa13q.com | google.com |

有些域名已被列入黑名单，有些是保护性注册的

- **1,516** homographic IDNs detected (100 blacklisted)
- Brands: few defensive registration

| Brand Domain | # Homographic IDN (% of 1,516) | # Defensive Registration |
|---|---|---|
| google.com | 121 (8.0%) | 19 |
| facebook.com | 98 (6.5%) | 0 |
| amazon.com | 55 (3.6%) | 14 |
| icloud.com | 42 (2.8%) | 0 |
| youtube.com | 41 (2.7%) | 0 |

可以批量生成攻击域名，绝大多数没有被注册

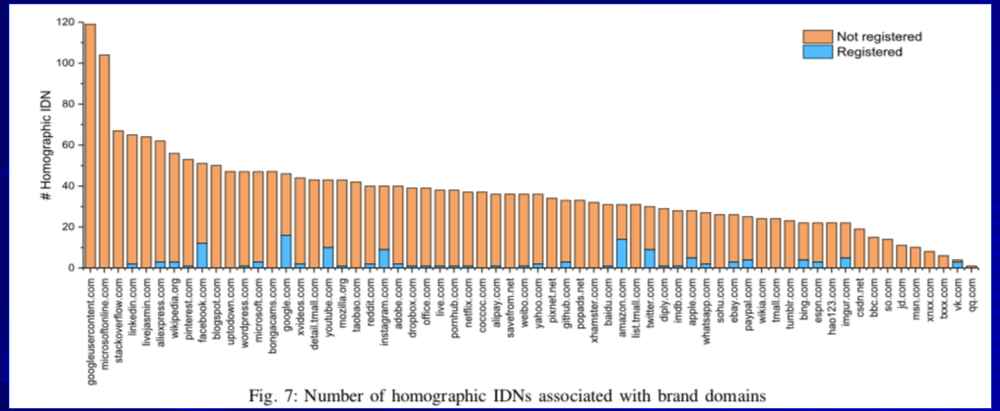
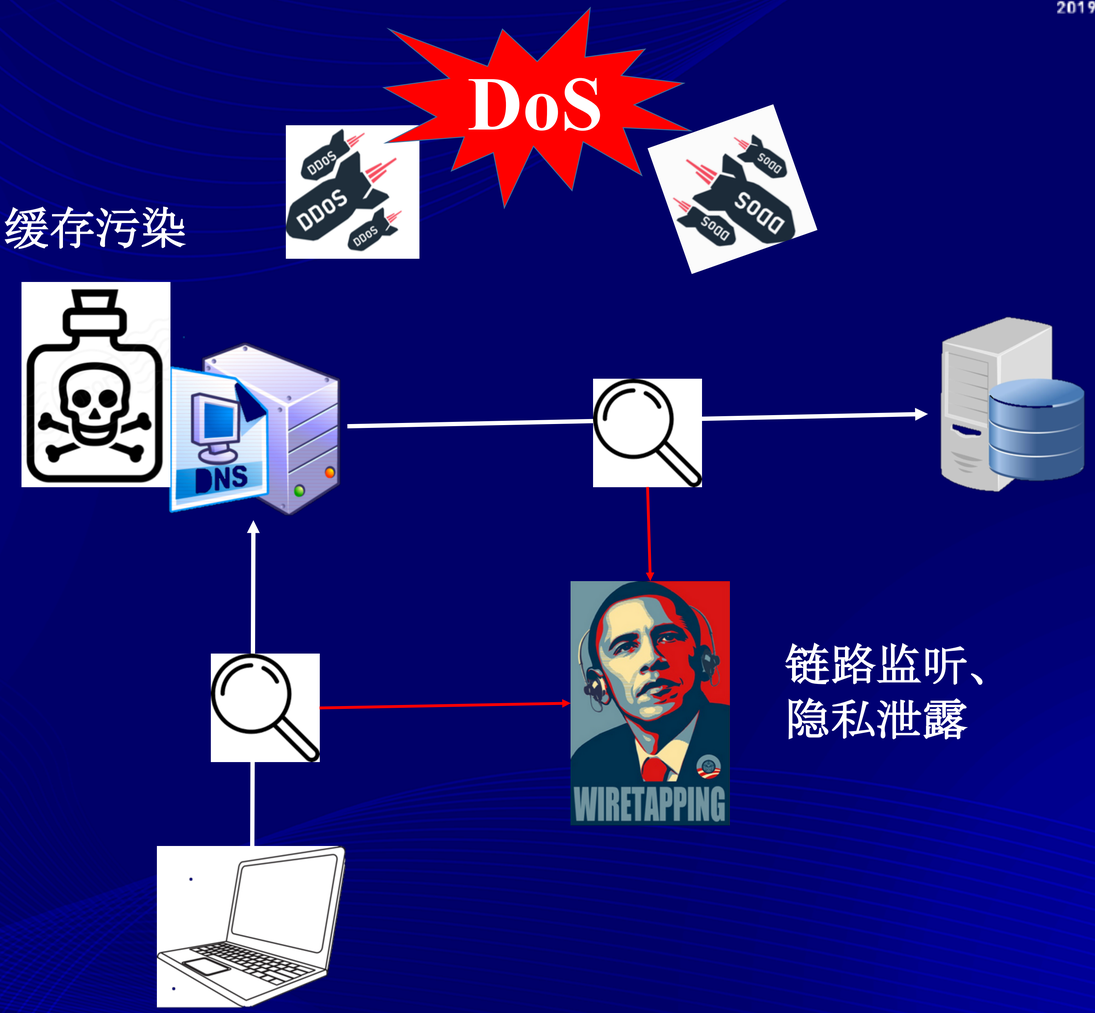



Fig. 7: Number of homographic IDNs associated with brand domains

- 为什么关注DNS安全？
- 根域名的历史和域名空间扩展
- **DNS协议攻击和协议安全的演进**

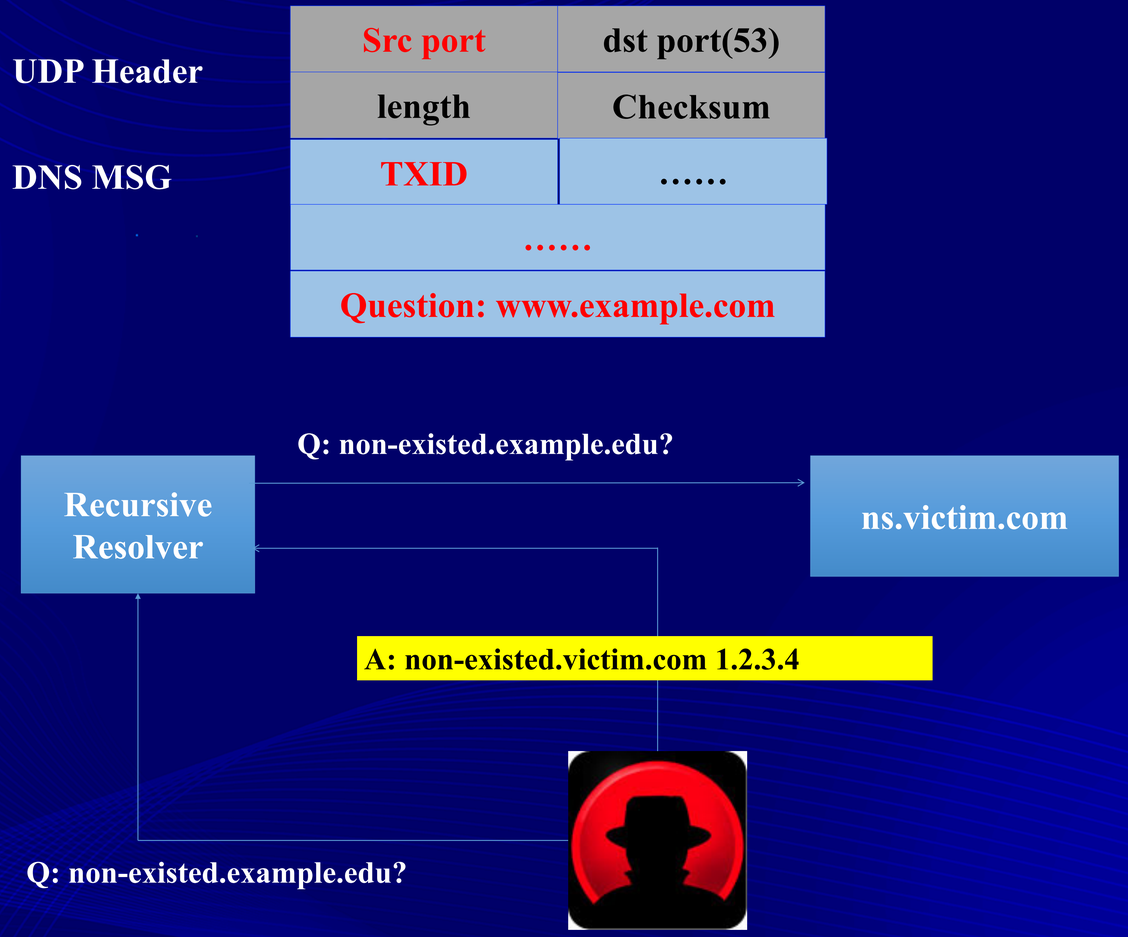
# DNS协议相关的安全问题

- 拒绝服务攻击DoS
- 缓存的污染
- 链路的劫持
- 流量的窃听/注入
- 利用DNS查询行为分析用户隐私信息



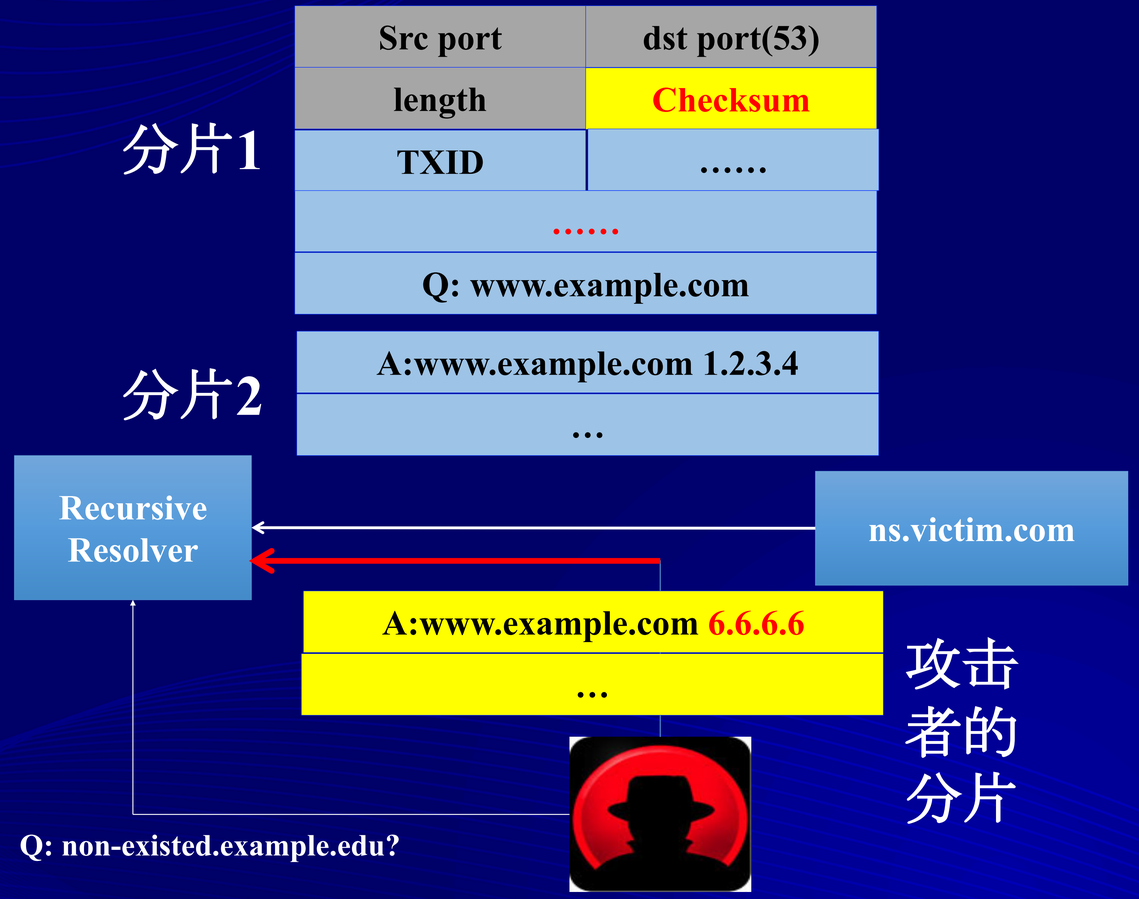
# Dan Kaminsky 缓存污染攻击及其防范(2008)

- 请求受攻击域名，伪造响应，
- 成功率本来：$1/2^{32}$，但是：
  - Src port： 可预测
  - TXID : 16 bit
  - 成功率：$1/2^{16}$
- 防范措施
  - Source Port :$2^{16}$
  - TXID Random: $2^{16}$
  - 0X20 encoding(2008)
  - 成功率：$2^{32+length}$



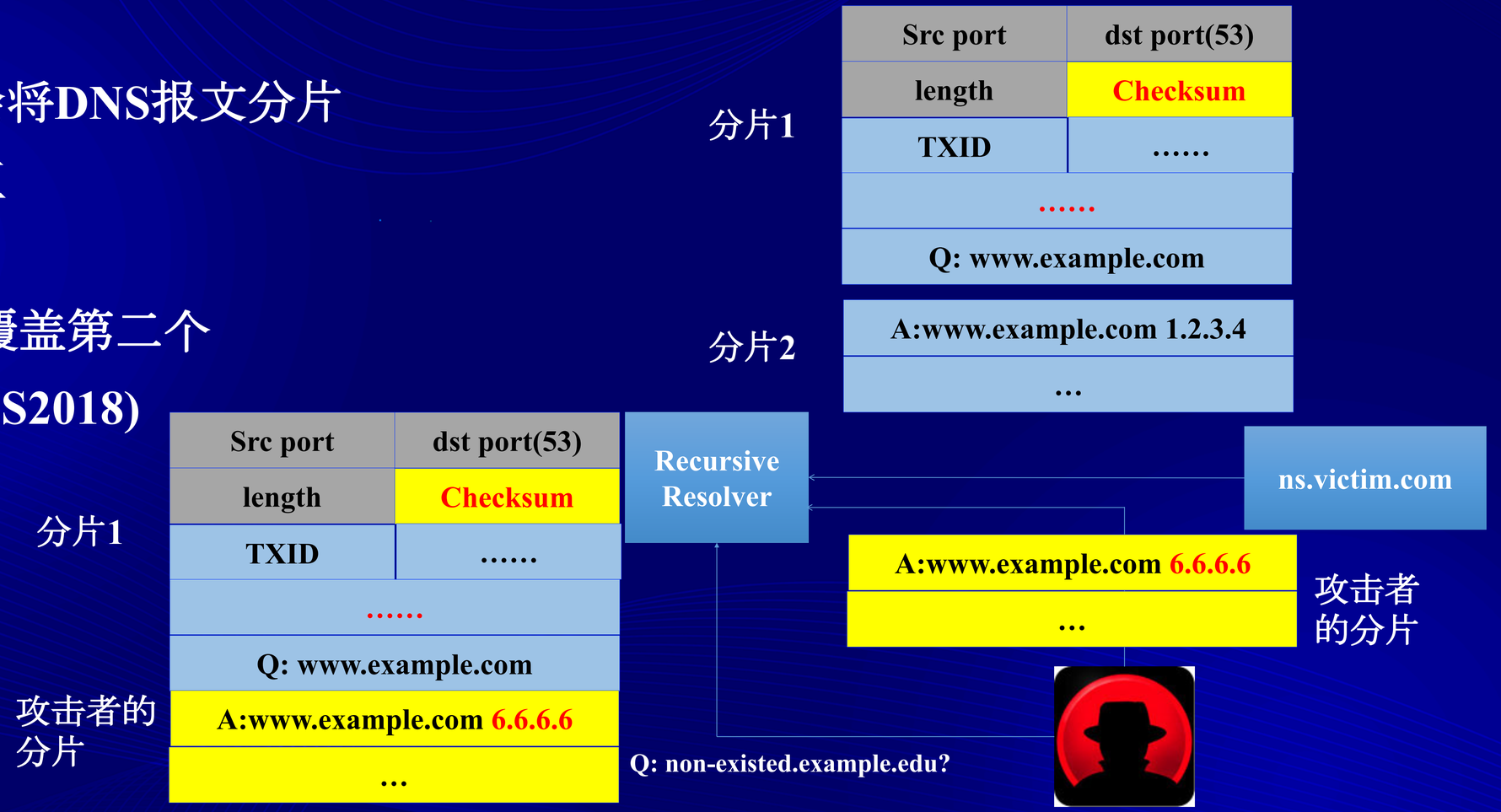
# 另一种缓存污染方法： UDP分片(Fragment)

- 服务器和网络设备可能会将DNS报文分片
- 第一个分片中含有随机值
- Checksum算法过于简单
- 攻击方法：让权威分片,覆盖第二个
- 例：攻击CA的DNS（CCS2018)



# 缓存污染方法： UDP分片(Fragment)

- 服务器和网络设备可能会将DNS报文分片
- 第一个分片中含有随机值
- Checksum算法过于简单
- 攻击方法：让权威分片,覆盖第二个
- 例：攻击CA的DNS（CCS2018)



# 新的缓存污染方法

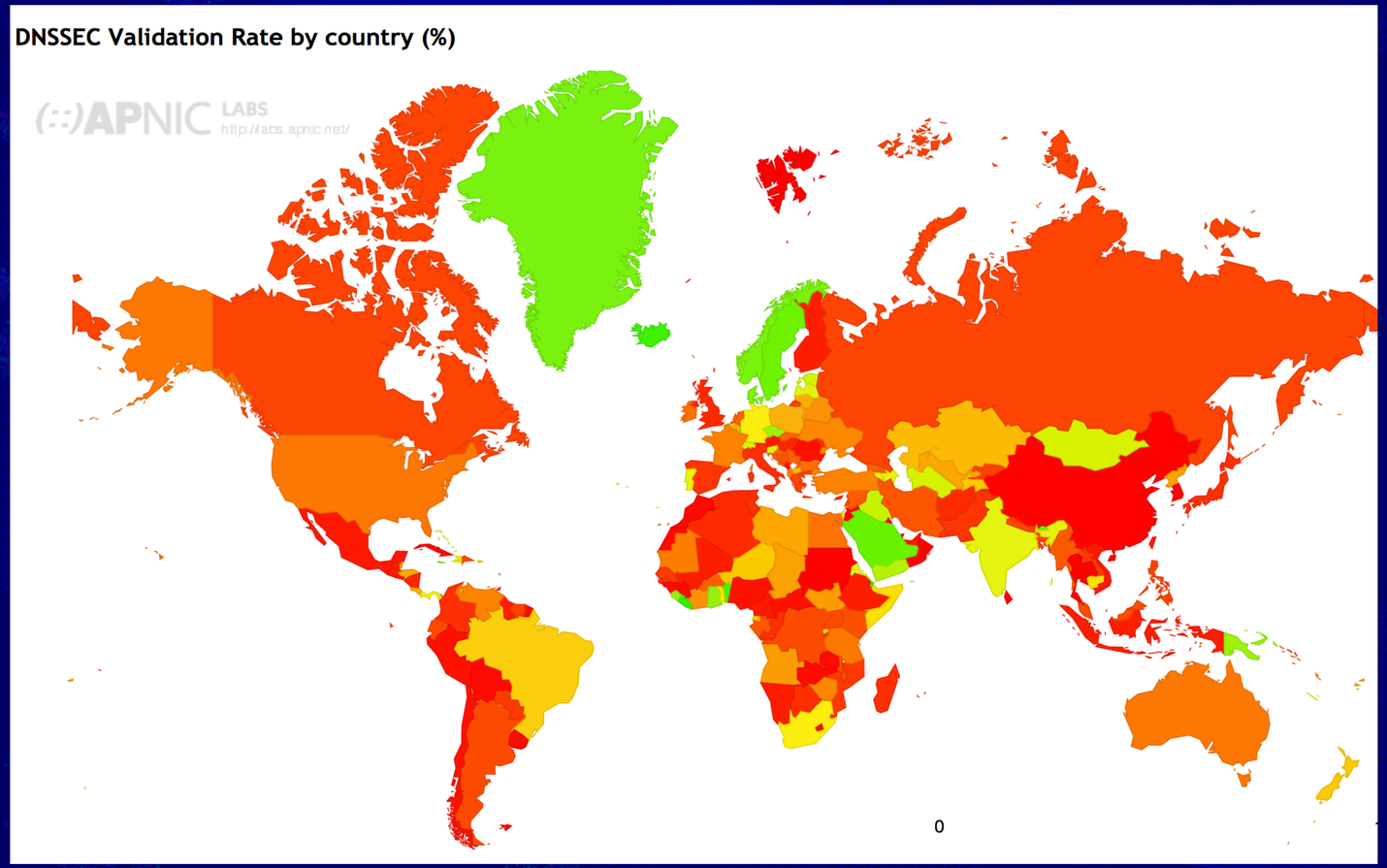
- 清华-奇安信联合实验室发现的新型DNS缓存污染攻击：构造超大的DNS请求，强迫服务器分片

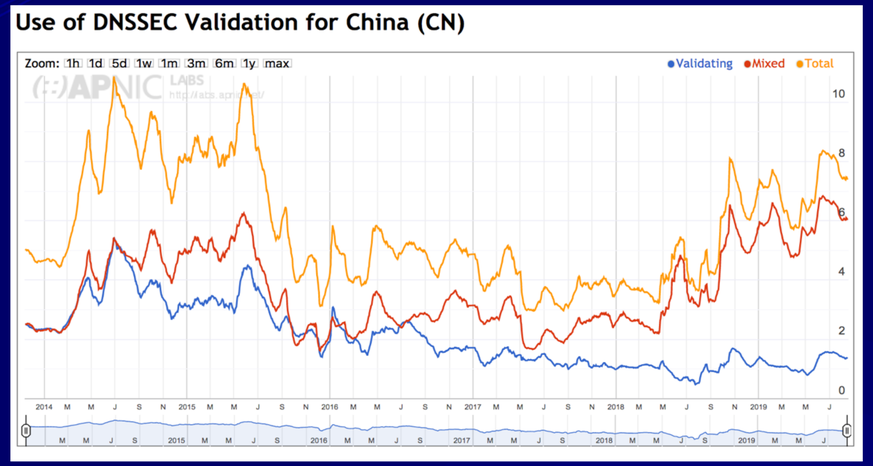


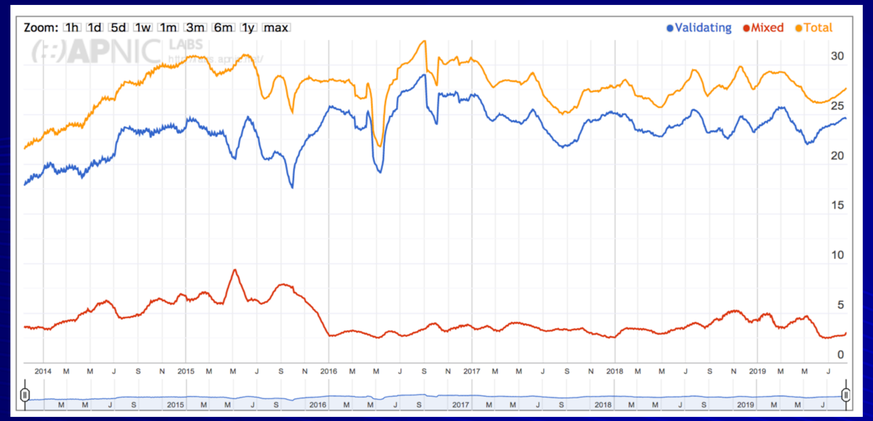
小米 飞鱼星 ASUS D-Link TP-LINK Tenda 腾达 motorola
HUAWEI MERCURY 水星 MerCruiser LINKSYS WAVLINK 睿因 FAST 迅捷 gee 极路由

# DNSSEC 验证的比例





# 中美三个行业权威服务器DNSSEC部署情况

| | 2018年8月测试结果 | | 2019年8月测试结果 | | |
|---|---|---|---|---|---|
| 域名类别 | 数量/比例 | 配置正确率 | 数量/比例 | 配置正确率 | |
| 中国国内银行 | 0/0 | NA | 0/0 | NA | |
| 美国国内银行 | 15/13% | 100% | 19/17% | 74% | ↓ |
| 中国政府gov.cn | 0/0 | 0 | 2/0.1% | 50% | ↑ |
| 美国政府gov | 1162/21% | 99.05% | 1141/21% | 97% | ↓ |
| 中国教育edu.cn | 32/0.4% | 0* | 61/2.6% | 61% | ↑ |
| 美国教育edu | 150/2% | 98.70% | 174/2.5% | 76% | ↓ |

# 加密DNS发展大事件

2009年
DNSCurve
第一个加密DNS协议草稿

2011年
DNSCrypt协议

2014年9月IETF
第一个DNS隐私工作组DPRIVE成立

2015年8月
RFC 7626
第一份讨论DNS隐私问题的RFC文档

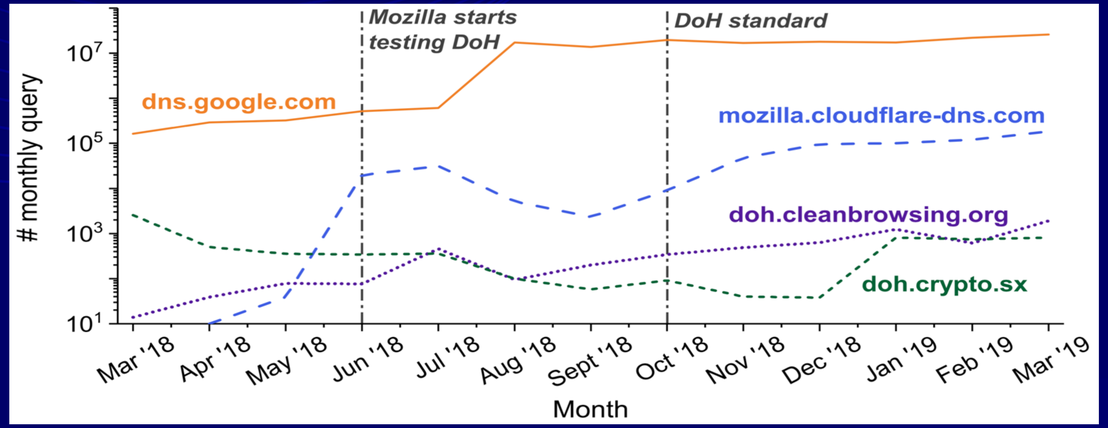
2016年5月
DNS-over-TLS (RFC 7858)
第一个被IETF标准化的加密DNS协议

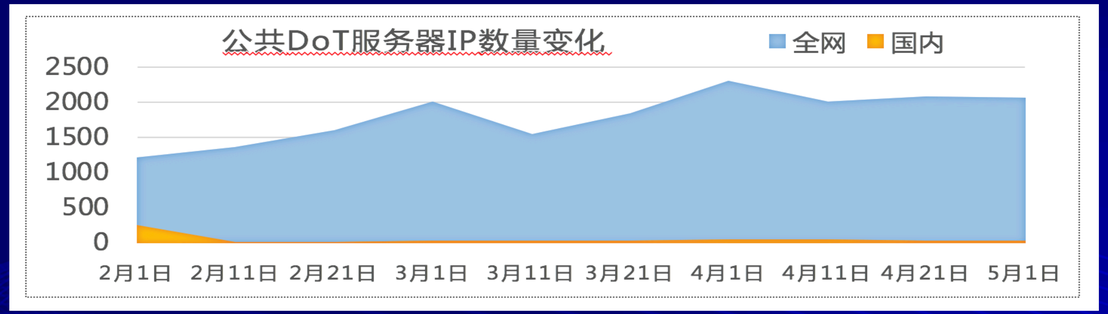
2017年9月
IETF DNS-over-HTTPS工作组成立

2018年10月
DNS-over-HTTPS (RFC 8484)
标准通过

# DoH的查询 & DOT 服务器的数量 （IMC2019）

- DoH查询：知名DoH服务占有较大比例
  - Google(8.8.8.8)
  - CloudFlare(1.1.1.1)
- 公共DNS-over-TLS解析服务器：1.5K~2K左右
  - 许多证书配置错误
- 中国的DoT DNS服务器部署很少
  - <50
- DNS加密仍然存在较大争议
- 加密DNS仍在缓慢增长

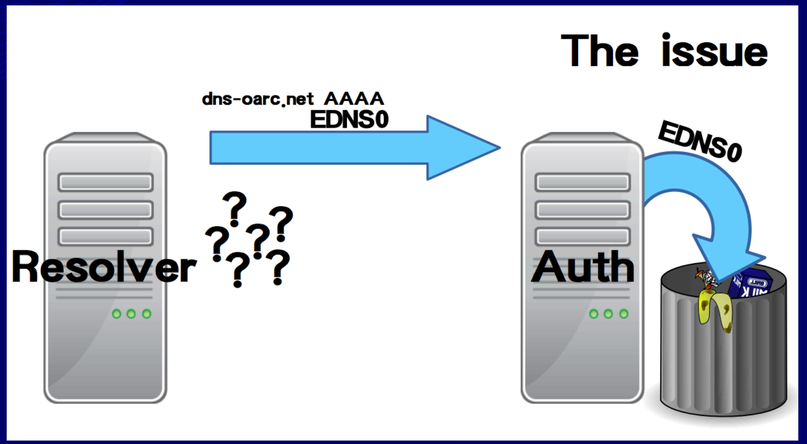


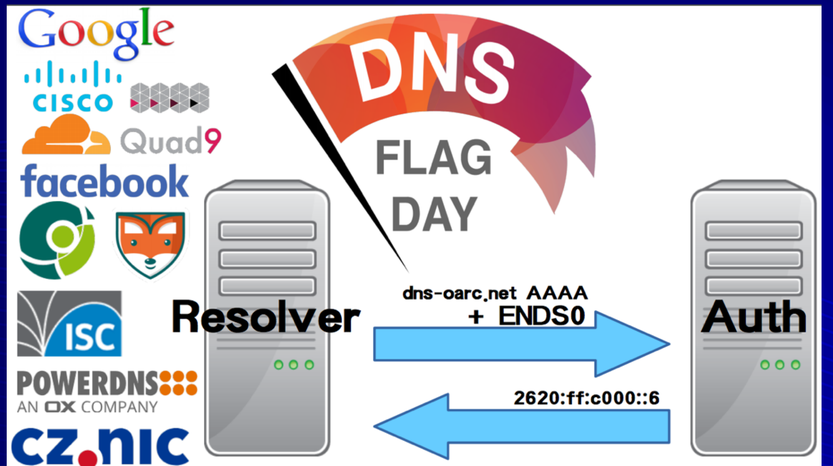




Chaoyi Lu and etc. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? IMC 2019

# EDNS和 DNS flag day

- 1987年的RFC 1035限制了DNS 报文的大小、新功能
- EDNS扩展DNS格式和功能
  - IPv6、DNSSEC、ECS等
  - 向后兼容的 Workaround尝试
  - 服务器不支持或被防火墙过滤
- DNS Flag day: dnsflagday.net
  - 2019/2/1日后，对EDNS实现不标准的授权服务器，Google等公共DNS将不再尝试访问，可能导致解析失败



# 2018年不支持EDNS 的Top 10 DNS 服务提供商

## Contacts needed! Top ten EDNS-broken providers

| provider domain | breakage | # broken |
|---|---|---|
| hichina.com. | 35.78 % | 469 611 |
| dnspod.com. | 25.66 % | 336 797 |
| myhostadmin.net. | 5.04 % | 66 208 |
| xincache.com. | 4.82 % | 63 246 |
| dnspod.net. | 3.27 % | 42 881 |
| dnsdun.net. | 2.85 % | 37 435 |
| gmoserver.jp. | 2.71 % | 35 595 |
| registrar-servers.com. | 1.64 % | 21 533 |
| alidns.com. | 1.63 % | 21 369 |
| metaregistrar.nl. | 1.20 % | 15 762 |

∑ 66 %

∑ 85 %

Top ten: EDNS-broken providers in October 2018

https://indico.dns-oarc.net/event/31/contributions/678/attachments/673/1102/dns_flag_day_panel.pdf

# 总结

- DNS功能远不止IP地址解析
- 了解DNS的历史有助于理解互联网治理现状，澄清某些认识
- DNS的问题仍然很多，DNS安全技术也在不断发展
- 与国际安全标准和最佳实践同步，提高互联网基础设施的内生安全能力

# THANKS