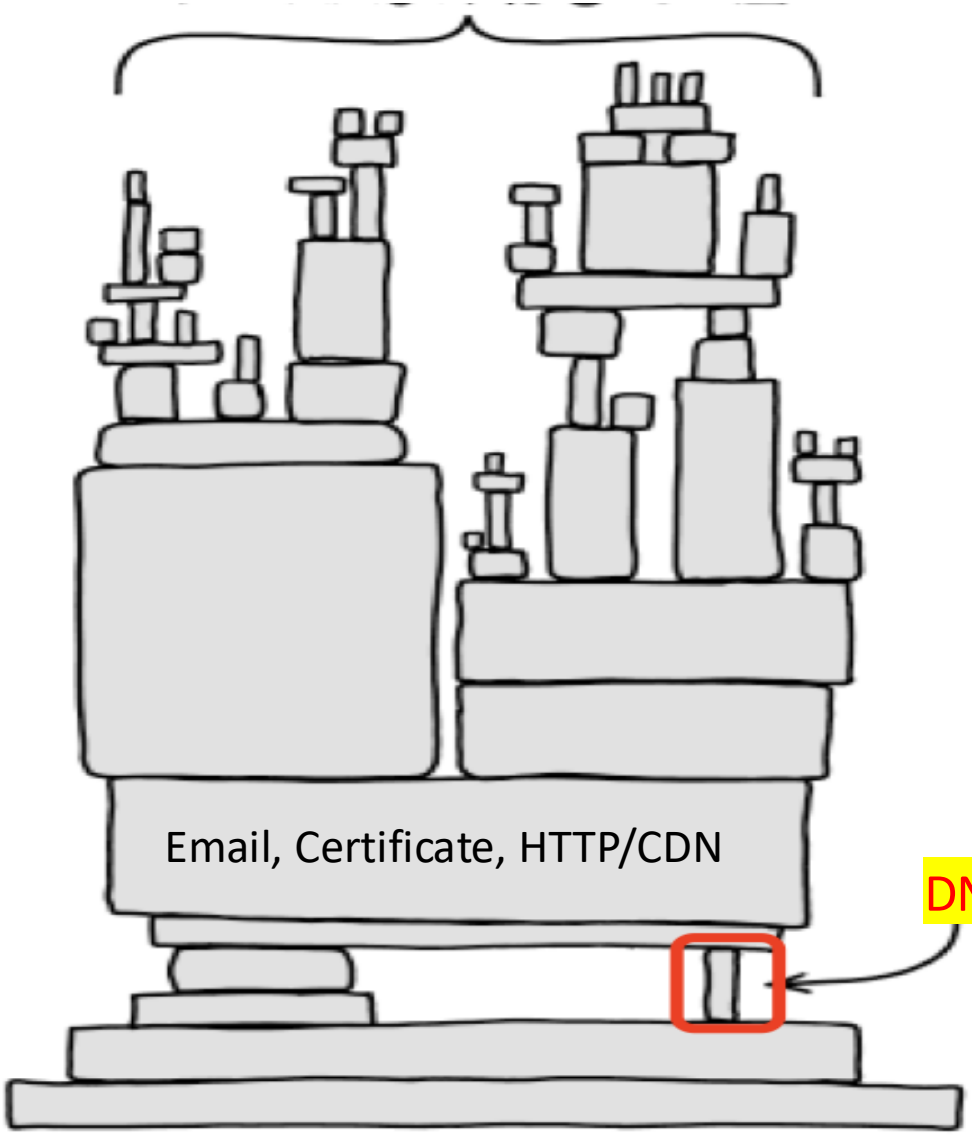
# DNS Security

Haixin Duan
Tsinghua University

# 目录

- DNS 重要攻击事件回顾
- DNS 服务的功能
- DNS 协议和工作原理
- DNS 的根及其治理
- 针对DNS 的攻击面
- DNS缓存污染攻击与防范
- DNS与反射放大攻击与防范

# 互联网应用



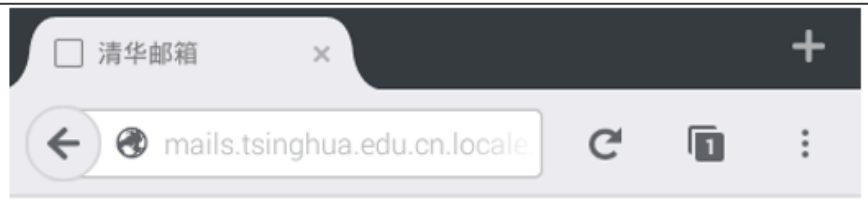
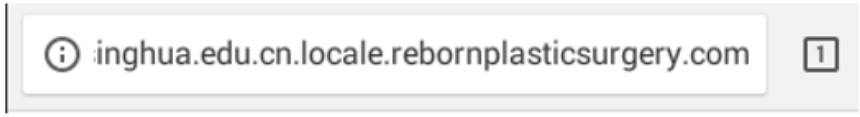
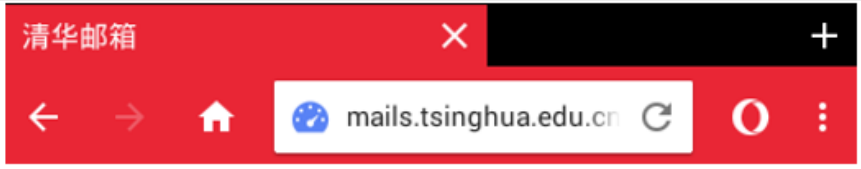
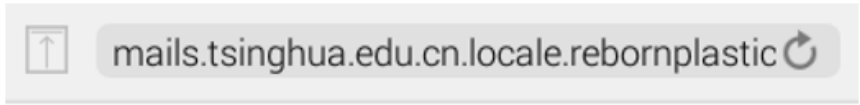

DNS 互联网的
阿喀琉斯之踵（Achilles' Heel）

# 清华邮箱里收到的邮件，点击链接

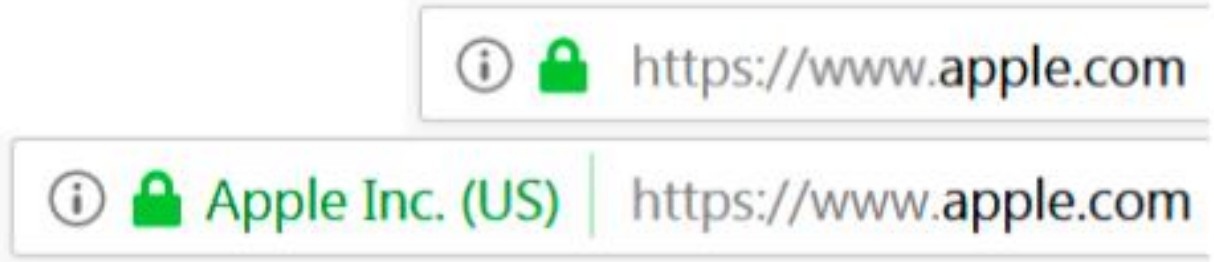

http://mails.tsinghua.edu...
mails.tsinghua.edu.cn.locale.rebornplasticsurgery.com
清华邮箱
清華大學 电子邮件系统
安全提示 | VPN设置 | 帮助 | English
用户登录
用户名：
@mail.tsinghua.edu.cn
登录密码：
忘记密码?
登录
Copyright © 2013 清华大学版权所有
如有问题请反馈到: support@tsinghua.edu.cn

We cannot even see URL address when we visit fake domain in mobile

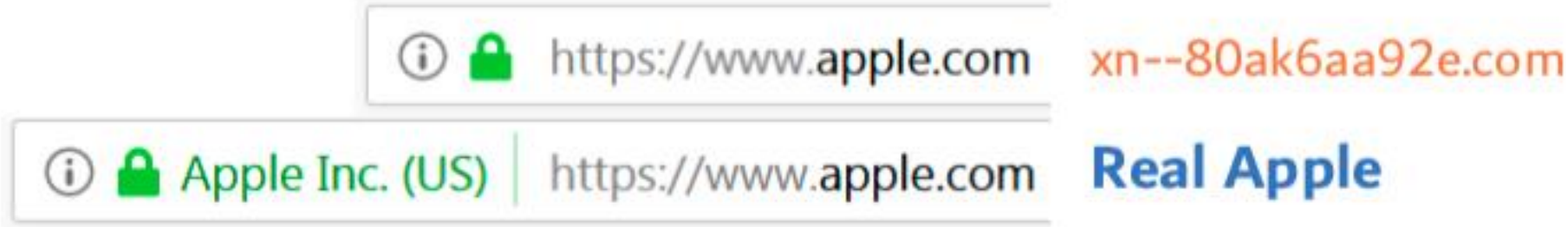


| Mobile (Resolution: 720x1280) | |
|---|---|
| **Browser Version** | **Address Bar** |
| Firefox 55.0 |   |
| Chrome 59.0.3071.125 |   |
| Opera 28.0.2254.119213 |   |
| Safari/537.36 |   |
| UC 11.7.2.954 |   |

# 利用域名进行钓鱼攻击



# 利用域名进行钓鱼攻击

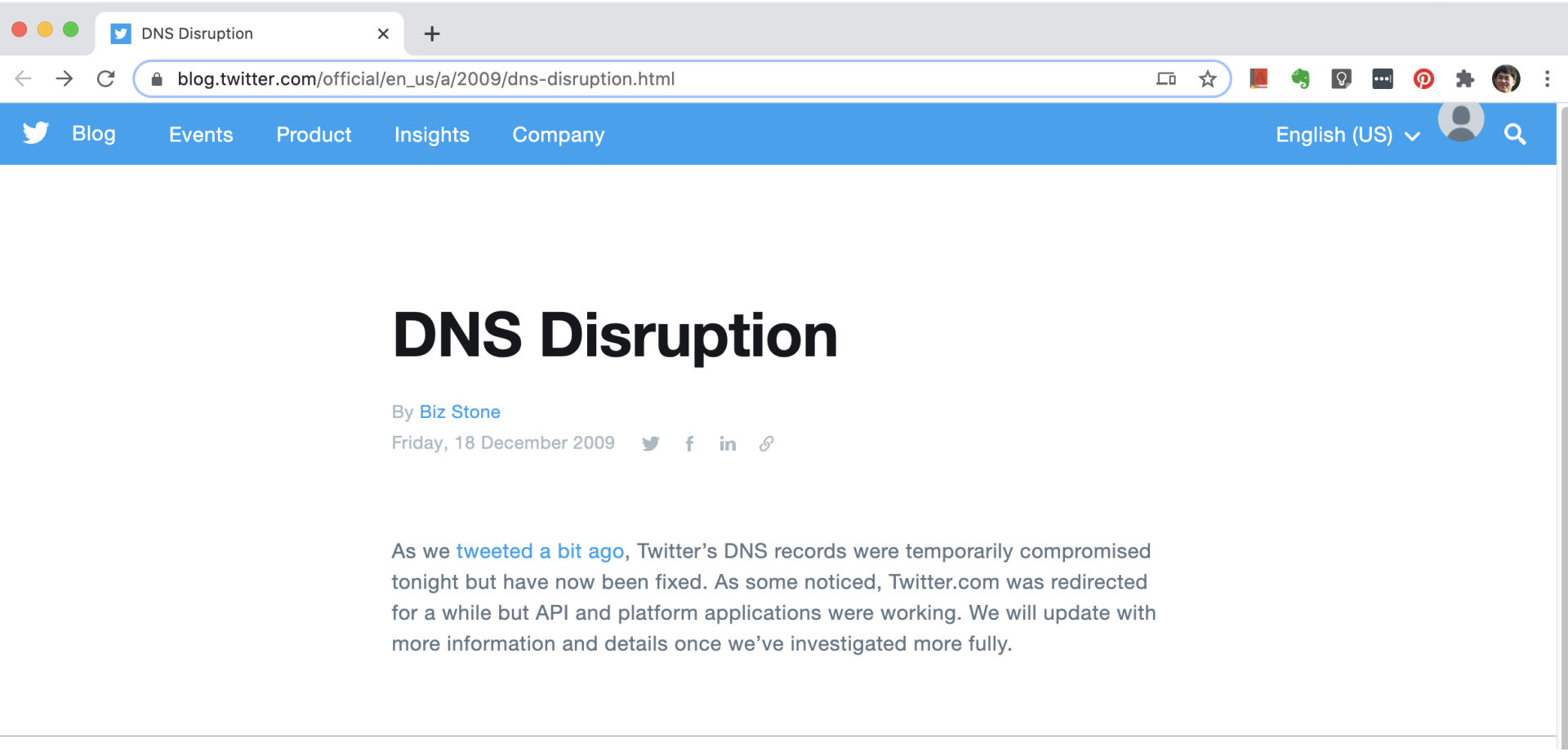




差点盗走十多亿，做空比特币又获利几十亿？黑客这一波到底干了什么？

https://zhuanlan.zhihu.com/p/34478534

# Twitter hacked, 2009/12/08




https://blog.twitter.com/official/en_us/a/2009/dns-disruption.html

# Report: Security Breach Behind Twitter Outage Did Not Originate with New Hampshire DNS Provider

**Wade Roush**
December 18th, 2009



A hacker attack on the domain name system (DNS) servers that enable access to Twitter's website disrupted service for many users late Thursday, directing them instead to a web page declaring "This site has been hacked by Iranian Cyber Army." In the wake of the attack, which was fended off within hours, many fingers are being pointed at Twitter's DNS provider, Manchester, NH-based Dyn Inc. But according to information obtained by Xconomy, the breach that apparently gave hackers access to the site did not occur at Dyn, and may in fact be traceable to a security hole at Twitter or at some other point of access.



The DNS is a global, distributed system that translates websites' familiar alphanumeric names, such as www.twitter.com, into Internet Protocol addresses that can be used by Web servers and Internet routers to deliver Web pages to people who request them. Many companies, including Twitter, outsource DNS services to specialized providers such as Dyn, whose computers are especially fast at resolving URLs into IP addresses. "The DNS is critical for the Internet infrastructure," says Phil Jacob, founder and CEO of Cambridge, MA-based product recommendation site Stylefeeder, which is also a Dyn client.

Jacob says Dyn executives filled him in today about the crisis at Twitter after he requested a briefing. From what he learned, he says, he is satisfied that the episode is not a sign of any weakness in Dyn's security procedures.

Kyle York, vice president of sales and marketing at Dyn, said he was limited in what he could say about the incident on the record. "This was an isolated incident," York says. "No unauthenticated user account accessed Twitter's Dynect Platform account. Dyn Inc is working with Twitter and the authories in an investigation on the issue."

Reading between the lines, York's statement would seem to suggest that Twitter's account at Dyn was accessed by hackers who appeared to have proper authorization—perhaps meaning a pilfered password. This apparently gave the hackers the ability to implement a "redirect" that caused Twitter's domain name to resolve, temporarily, to an incorrect Internet address (the address of the Iranian Cyber Army page).

Reading between the lines, York's statement would seem to suggest that Twitter's account at Dyn was accessed by hackers who appeared to have proper authorization—perhaps meaning a pilfered password. This apparently gave the hackers the ability to implement a "redirect" that caused Twitter's domain name to resolve, temporarily, to an incorrect Internet address (the address of the Iranian Cyber Army page).

The hackers did not have access to any other account, York said. "At no time was DNS not resolving on the global network. This was an isolated incident just to Twitter, not a problem that affected any other Dyn users."

Stylefeeder's Jacob said he wasn't satisfied after reading media accounts of the outage this morning. "I saw this news this morning, and I was like,'Whoa, what's up with that?,' because Stylefeeder uses Dynect [Dyn's DNS platform] and obviously, since this is the holiday shopping season, something like that happening to us would not be favorable," Jacob says. "I immediately contacted [Dyn], and they provided me with extra information that is not publicly available, because I am a Dynect customer. And without violating other clients' confidentiality, they gave me some extra insight into what occurred, which to my mind, put to rest that the problem lay not with Dynect but elsewhere—but not necessarily with Twitter."

"I don't think that this story is being well told," Jacob continues. "The press today is basically saying that Twitter had a DNS problem, and here is their DNS provider, so it's their fault. And that is not actually the case."

Jacob said he has no information about the exact chain of events that led to the compromise. But he suggested that it might be the result of lax security standards at Twitter, perhaps a holdover from the young company's early days as a startup undergoing rapid growth.

"While I understand that it's hard for a growing organization to make sure their systems are secured properly, I think that Twitter is at the point now of being a top-10 website, where they ought to be able to avoid problems like this, especially given the resources they have," Jacob said.

At the same time, he said, "I would feel strongly about noting that the people who are running Twitter now are very capable, and this is unfortunately just one of those holes that they probably didn't yet get around to fixing."

A spokesperson for Twitter didn't immediately respond to a request for comment.

https://xconomy.com/boston/2009/12/18/report-security-breach-behind-twitter-outage-did-not-originate-with-new-hampshire-dns-provider/?single_page=true

# 同样的攻击

- Deface the website of a domain
  - baidu.com Jan. 12,2010, 7:40am -18:00pm

# 百度就黑客事件起诉美国企业

2010年1月20日


谷歌刚好在百度遭到攻击当天宣布可能从中国撤资。

**中国互联网搜索引擎巨头百度宣布向美国一家域名注册商提出起诉，就百度网站上周遭到黑客瘫痪事件索赔。**

百度星期三（1月20日）发表声明说，该公司已经在美国纽约某法院对Register.com有限公司提出起诉，并考虑把百度域名迁回中国管理。

百度表示，他们认为是管理全球超过250万个域名的Register.com存在"重大疏忽"导致百度网站的域名遭到"非法和恶意改动"。

就在百度网站遭到攻击的同一天，美国搜索引擎巨头谷歌声称遭受针对中国人权活动分子"复杂精密的"网络攻击，威胁关闭其在华业务。

消息为百度在美国纳斯达克交易所挂牌交易的股份价格带来支持，上周五（15日）更一度创下每股470.25美元的纪录。

百度网站上周二（12日）遭到自称是伊朗网军（Iranian Cyber Army）的黑客攻击，导致百度网站瘫痪数小时。

百度的声明没有交代索赔金额，其发言人也拒绝透露诉讼的进一步详情。

在百度遭到攻击后翌日，伊朗也有网站遭到黑客攻击，被怀疑是中国黑客的报复行为。当时百度发表声明，表示不认同这种出于"义愤"的还击，呼吁中国网民冷静。

http://www.sina.com.cn 2010年02月25日 14:55 新浪科技

新浪科技讯 北京时间2月25日下午消息，据国外媒体今日报道，美国一家法院日前披露了百度(NasdaqGS:BIDU)起诉美国域名注册商Register.com的起诉书内容。

起诉书显示，一名黑客上月假冒百度工作人员通过网络聊天工具与Register.com取得联系，并借此入侵了百度的账号，从而导致百度数小时无法访问。

百度在起诉文件中表示，在Baidu.com域名被重新定向至一个声称"This site has been hacked by the Iranian Cyber Army"(该网站被伊朗网络部队黑了)的页面后，百度最初就此事与Register.com的客服人员取得联系时，对方拒绝为百度提供帮助。该起诉书于上月递交给美国纽约南区地方法院，但该法院直到最近才公布了完整的副本。

起诉书称，由于遭到黑客攻击，百度的服务中断了5小时，并因此产生了数百万美元的收入损失和其他成本。

百度表示，本次攻击始于1月11日下午，当时黑客通过网络聊天工具假冒百度员工向Register.com的客服人员求助。黑客要求客服代表更改百度的电子邮件地址存档。尽管这名黑客并未正确回答安全问题，但该客服代表随后仍然向百度的邮箱发送了确认码。

百度的起诉书显示，由于黑客无法访问百度的电子邮箱，所以他编造了一个确认码，并在客服代表索取时将其发送给对方。在没有对两组代码进行比对的情况下，这名客服代表便将对方的虚假答案视为正确答案，并同意了黑客的请求，将百度的电子邮件地址存档更改为"antiwahabi2008@gmail.com"。

百度在起诉书写道："在申请人无法进行正确的安全验证，甚至两次提供错误信息的情况下，Register.com便将存档的电子邮件从一个包含账户所有者用户名的企业地址，改成了一个含有明显政治信息(antiwahabi)、而且使用百度竞争对手域名(gmail.com)的地址。这简直令人难以置信。"

目前还不清楚"antiwahabi"的具体意义，但其拼写与一个名为瓦哈比穆斯林(Wahabi Muslim)的宗教派别相吻合。百度尚未对此置评。

百度的起诉书显示，该黑客随后利用专为忘记密码的用户设计的"重设密码"功能，要求Register.com向更改后的电子邮件地址发送了百度账号的新密码。这名黑客随后还更改了百度账号的设置，并将访问者引导至另外一个网站，整个过程耗时不足一个小时。

Register.com尚未对此置评，但该公司上月曾表示，百度的起诉"毫无根据"，并承诺将配合执法部门的调查。

Register.com等域名注册商的业务是出售域名(例如Baidu.com)，并为用户提供必要的设置，将访问者引导至正确的网站。

百度起诉书的完整副本最早由域名信息网站Domain Name Wire发布，该网站编辑安德鲁·阿尔曼(Andrew Allemann)说："这就好比有人问你社会保险账号的后四位数，而你随便编了一个，但对方并未进行验证。"他认为，如果域名注册服务机构要求对方出示额外的证明信息，便可避免这一攻击。

此前也曾发生过类似的攻击。例如，一名黑客2008年入侵了电子支付服务供应商CheckFree的账号，并修改了该公司的域名信息。阿尔曼说："可惜的是，在事情发生到自己

https://www.bbc.com/zhongwen/simp/business/2010/01/100120_baidu_lawsuite

# 美国法院批准百度继续起诉域名服务商Register



2010-07-26 14:27:46 出处：快科技 作者：萧萧 编辑：萧萧 人气：3199 次 评论(16)

默认

日前，美国纽约曼哈顿联邦法院批准了百度对其美国域名服务供应商Register.com的起诉，但是却驳回了百度所提出的7项指控中的5项，包括商标侵权和交所协助非法入侵等。

这起诉讼始于今年1月份，百度一纸诉状将Register.com告上法庭。在起诉中中，百度表示，北京时间2010年1月12日，由于Register.com的重大疏忽，百度的域名解析遭到不法分子恶意篡改，导致全球多处用户不能访问百度网站，故障持续数小时，给百度造成了严重的损失。

曼哈顿法院虽然驳回了百度提出的5项指控，不过法院允许百度继续指控Register.com违反合同以及严重疏忽和行为不当，以违反安全为由索取赔偿。


# Register.com settles Baidu domain hijacking lawsuit

Kevin Murphy, November 25, 2010, 14:28:53 (UTC), Domain Registrars

**Register.com has apologised to Chinese portal company Baidu for allowing its domain, baidu.com, to be hijacked by the Iranian Cyber Army hacker group.**

The two companies have announced that the lawsuit, which alleged gross negligence among other things, has now been settled. Terms were not disclosed.

If Baidu's complaint was to be believed, the hackers took over baidu.com with a trivial social engineering attack that relied upon a Register.com tech support employee being asleep at the wheel.

The company is one of China's largest internet firms, employing over 6,000 people and turning over well over $600 million a year. But for the period of the hijack, visitors to baidu.com instead just saw the hackers' defacement message instead.

The registrar had argued in court that its terms and conditions released it from liability, but the judge didn't buy it.

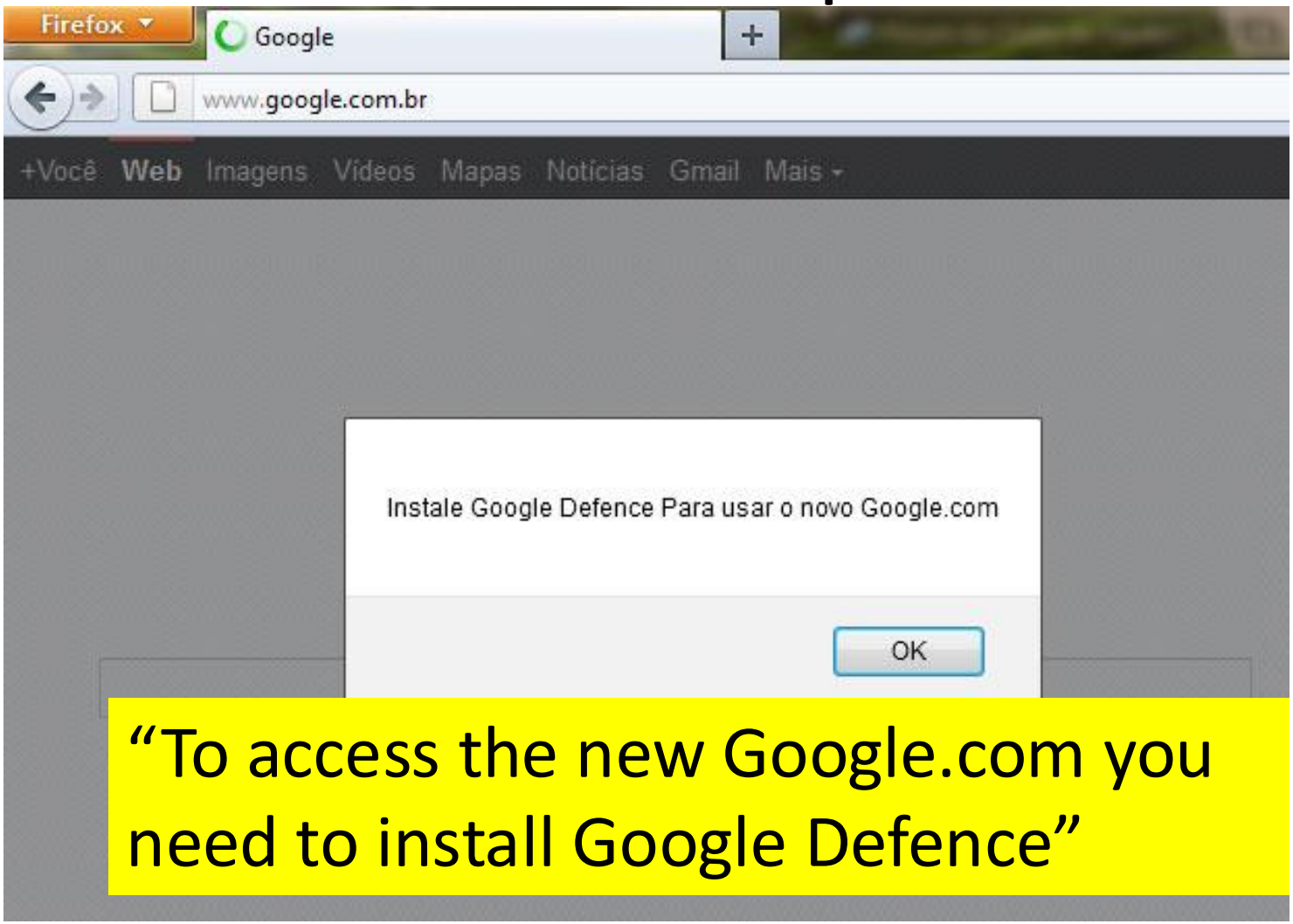
Register.com, which was acquired by Web.com for $135 million in June, said yesterday:

> After an internal investigation, we found that the breach occurred because Register's security protocols had been compromised. We have worked with United States law enforcement officials and Baidu to address the issue. We sincerely apologize to Baidu for the disruption that occurred to its services as a result of this incident.

Baidu said it accepted the apology. And the check, I imagine.

http://domainincite.com/2752-register-com-settles-baidu-domain-hijacking-lawsuit

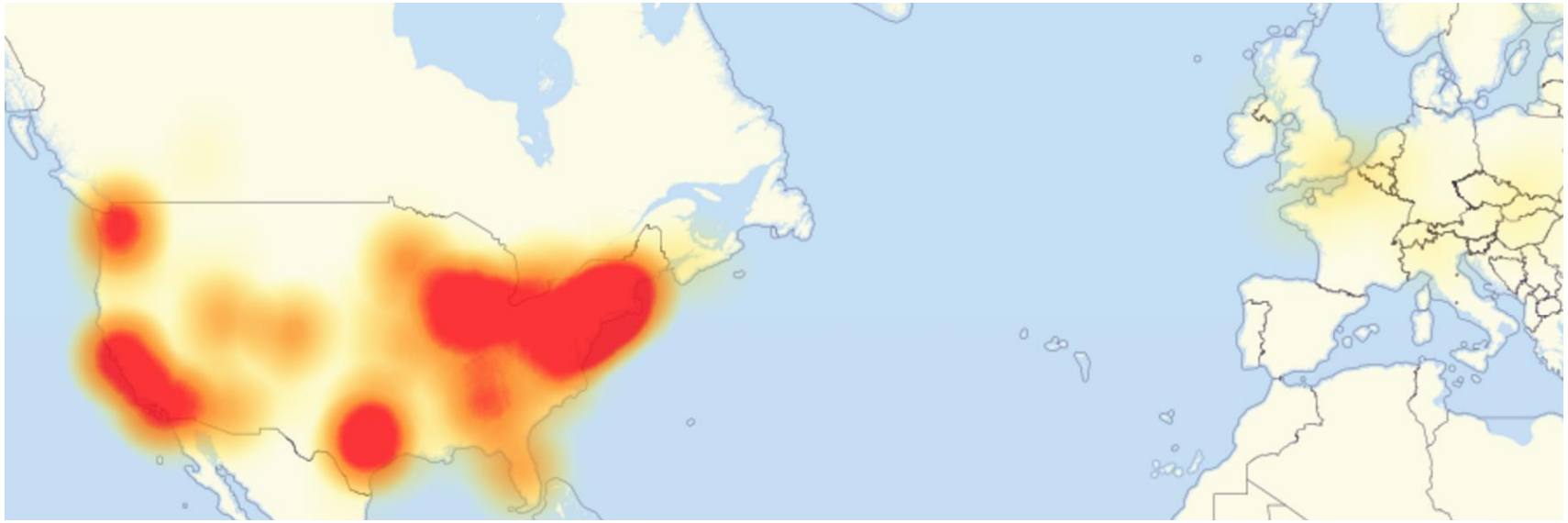
# Brazillian ISP's DNS cache poisoned 2011




http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil

# Dyn cyberattack, 2016

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack



- Airbnb[11]
- Amazon.com[8]
- Ancestry.com[12][13]
- *The A.V. Club*[14]
- BBC[13]
- *The Boston Globe*[11]
- Box[15]
- *Business Insider*[13]
- CNN[13]
- Comcast[16]
- CrunchBase[13]
- DirecTV[13]
- *The Elder Scrolls Online*[13][17]
- Etsy[11][18]
- FiveThirtyEight[13]
- Fox News[19]
- *The Guardian*[19]
- GitHub[11][16]
- Grubhub[20]
- HBO[13]
- Heroku[21]
- HostGator[13]
- iHeartRadio[12][22]
- Imgur[23]
- Indiegogo[12]
- Mashable[24]
- National Hockey
- Netflix[13][19]
- *The New York Times*[11][16]
- Overstock.com[13]
- PayPal[18]
- Pinterest[16][18]
- Pixlr[13]
- PlayStation Network[16]
- Qualtrics[12]
- Quora[13]
- Reddit[12][16][18]
- Roblox[25]
- Ruby Lane[13]
- *RuneScape*[12]
- SaneBox[21]
- Seamless[23]
- *Second Life*[26]
- Shopify[11]
- Slack[23]
- SoundCloud[11][18]
- Squarespace[13]
- Spotify[12][16][18]
- Starbucks[12][22]
- Storify[15]
- Swedish Civil Contingencies Agency[27]
- Swedish Government[27]
- Tumblr[12][16]
- Twilio[12][13]
- Verizon Communications[16]
- Visa[28]
- Vox Media[29]
- Walgreens[13]
- *The Wall Street Journal*[19]
- Wikia[12]
- *Wired*[15]
- Wix.com[30]
- WWE Network[31]
- Xbox Live[32]
- Yammer[23]
- Yelp[13]
- Zillow[13]

# Dyn Attacker Motives

The New York Times

"It is possible, investigators say, that the attack on Dyn was conducted by a criminal group that wanted to extort the company. Or it could have been done by "hacktivists." Or a foreign power that wanted to remind the United States of its vulnerability."

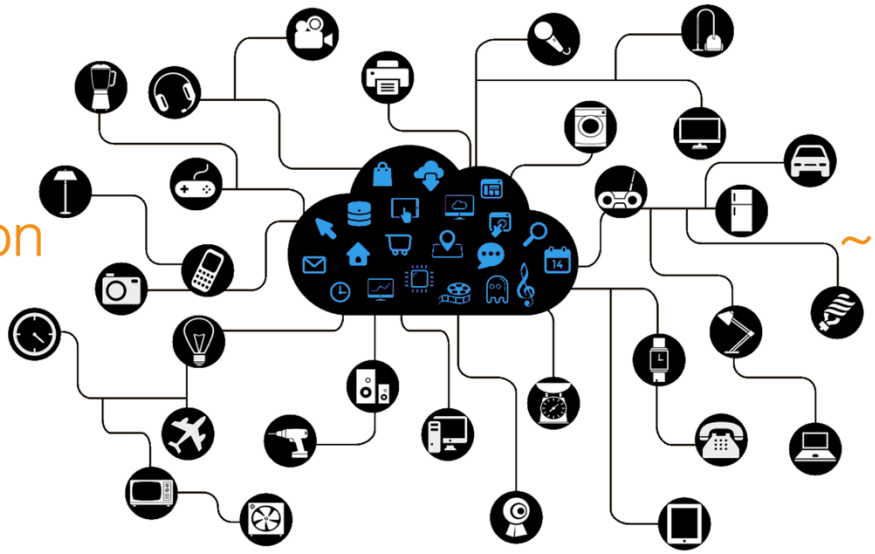
reddit amazon web services NETFLIX Spotify twitter GitHub PayPal

| Targeted IP | rDNS | Passive DNS |
|---|---|---|
| 208.78.70.5 | ns1.p05.dynect.net | **ns00.playstation.net** |
| 204.13.250.5 | ns2.p05.dynect.net | **ns01.playstation.net** |
| 208.78.71.5 | ns3.p05.dynect.net | **ns02.playstation.net** |
| 204.13.251.5 | ns4.p05.dynect.net | **ns03.playstation.net** |
| 198.107.156.219 | service.playstation.net | **ns05.playstation.net** |
| 216.115.91.57 | service.playstation.net | **ns06.playstation.net** |

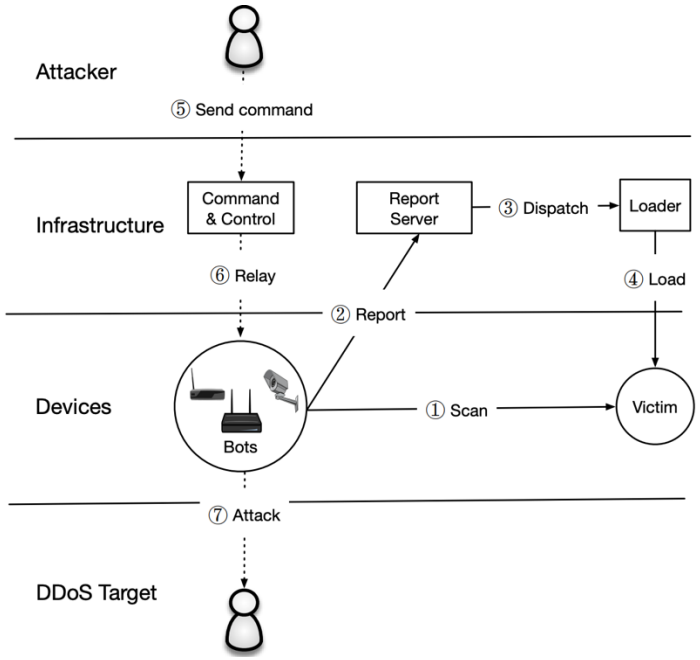
- Top targets are linked to Sony PlayStation
- Attacks on Dyn interspersed among attacks on other game services

# Growing IoT Threat

**2016**
6 - 9 Billion



**2020**
~30 Billion



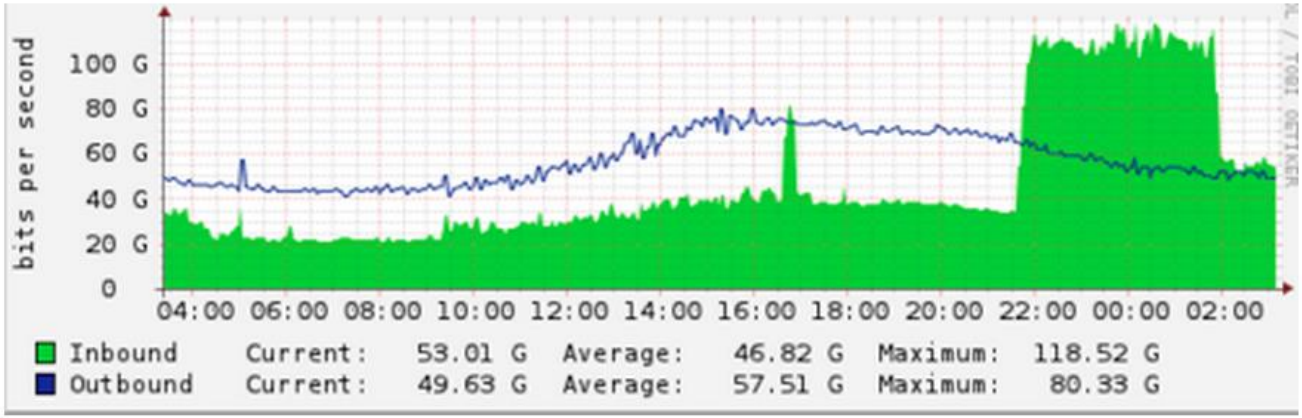

| Data Source | Size |
|---|---|
| Network Telescope | 4.7M unused IPs |
| Active Scanning | 136 IPv4 scans |
| Telnet Honeypots | 434 binaries |
| Malware Repository | 594 binaries |
| Active/Passive DNS | 499M daily RRs |
| C2 Milkers | 64K issued attacks |
| Krebs DDoS Attack | 170K attacker IPs |
| Dyn DDoS Attack | 108K attacker IPS |

**July 2016 - February 2017**

# DNS 被用作网络攻击的武器

blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho

attack is picking up again.




**How to Generate a 75Gbps DDoS**

The largest source of attack traffic against Spamhaus came from DNS reflection. I've written about these attacks before and in the last year they have become the source of the largest Layer 3 DDoS attacks we see (sometimes well exceeding 100Gbps). Open DNS resolvers are quickly becoming the scourge of the Internet and the size of these attacks will only continue to rise until all providers make a concerted effort to close them. (It also makes sense to implement BCP-38, but that's a topic for another post another time.)

The basic technique of a DNS reflection attack is to send a request for a large DNS zone file with the source IP address spoofed to be the intended victim to a large number of open DNS resolvers. The resolvers then respond to the request, sending

# 国家域名解析节点遭受史上最大规模DDOS攻击

2013年08月25日 09:10 作者: [字号：大 中 小] 打印

8月25日凌晨零时左右，国家域名解析节点受到拒绝服务攻击，经中国互联网络信息中心处置，至2时许，服务恢复正常，凌晨3时通过官微发出通告。凌晨4时许，国家域名解析节点再次受到有史以来最大规模的拒绝服务攻击，部分网站解析受到影响，导致访问缓慢或中断。至发出通告时，攻击仍在持续，国家域名解析服务已逐步恢复。

工业和信息化部启动了"域名系统安全专项应急预案"，进一步保障国家域名的解析服务。中国互联网络信息中心对受到影响的用户表示歉意，对发动网络攻击影响互联网稳定的行为表示谴责。中国互联网络信息中心将与国家各部门协同，继续提升服务能力。

分享按钮

联系我们

服务电话 010--58813000

通讯地址：北京中关村南四街四号中国科学院软件园1号楼一层

邮政地址：北京349信箱6分箱 CNNIC

邮政编码：100190

传　　真：010-58812666

网　　址：www.cnnic.cn

中国互联网络信息中心.中国

电子邮件：service@cnnic.cn(服务邮箱)

supervise@cnnic.cn(投诉邮箱)

依托科技创新 构建网络边防 维护网络主权

# 人民日报权威论坛：从网络大国走向网络强国

王远

2014年06月24日02:57 来源：人民网-人民日报 手机看新闻



原标题：从网络大国走向网络强国（权威论坛）

# 伊拉克、利比亚的域名“消失”

王军：目前美国掌握着全球互联网13台域名根服务器中的10台。理论上，只要在根服务器上屏蔽该国家域名，就能让这个国家的国家顶级域名网站在网络上瞬间“消失”。在这个意义上，美国具有全球独一无二的制网权，有能力威慑他国的网络边疆和网络主权。譬如，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。2004年4月，由于在顶级域名管理权问题上发生了分歧，利比亚顶级域名“.ly”瘫痪，利比亚诸多官方网站在互联网上消失了3天。2009年5月30日，微软遵照美国政府的意志，将古巴、伊朗、叙利亚、苏丹和朝鲜5国互联网用户的聊天软件“微软网络服务”（MSN）关闭。一些国家为了防止美国瘫痪自己的顶级域名，在技术上积极攻关，进而形成了替代性的国内网络服务体系，可以在美国停止网络域名解析后，使该国网络依然能在国家范围内系统运行，但不与国外网络链接。

# 2021年6月，美国司法部查封36个伊朗媒体域名

- **部分被查封域名**
  - 伊朗英文电视台 presstv.com
  - 伊朗世界新闻卫视 alalamtv.net
- **查封的法律依据**
  - “违反美国的制裁措施”
  - “传播针对美国的虚假消息”


域名 presstv.com
被查封后的网站 主页

# 2020年10月，美国查封92个伊朗革命卫队域名

- **域名被查封的理由**
  - “从事虚假宣传活动”
  - “影响美国国内和外交政策”

我们将继续使用一切工具，阻止伊朗政府滥用美国公司和社交媒体进行政治宣传活动，试图秘密影响美国公众并挑拨离间。

--国家安全助理司法部长

THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT | OUR AGENCY | TOPICS | NEWS | RESOURCES | CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Wednesday, October 7, 2020

**United States Seizes Domain Names Used by Iran's Islamic Revolutionary Guard Corps**

**Seizure Documents Describe Iranian Government's Efforts to Use Domains as Part of Global Disinformation Campaign**

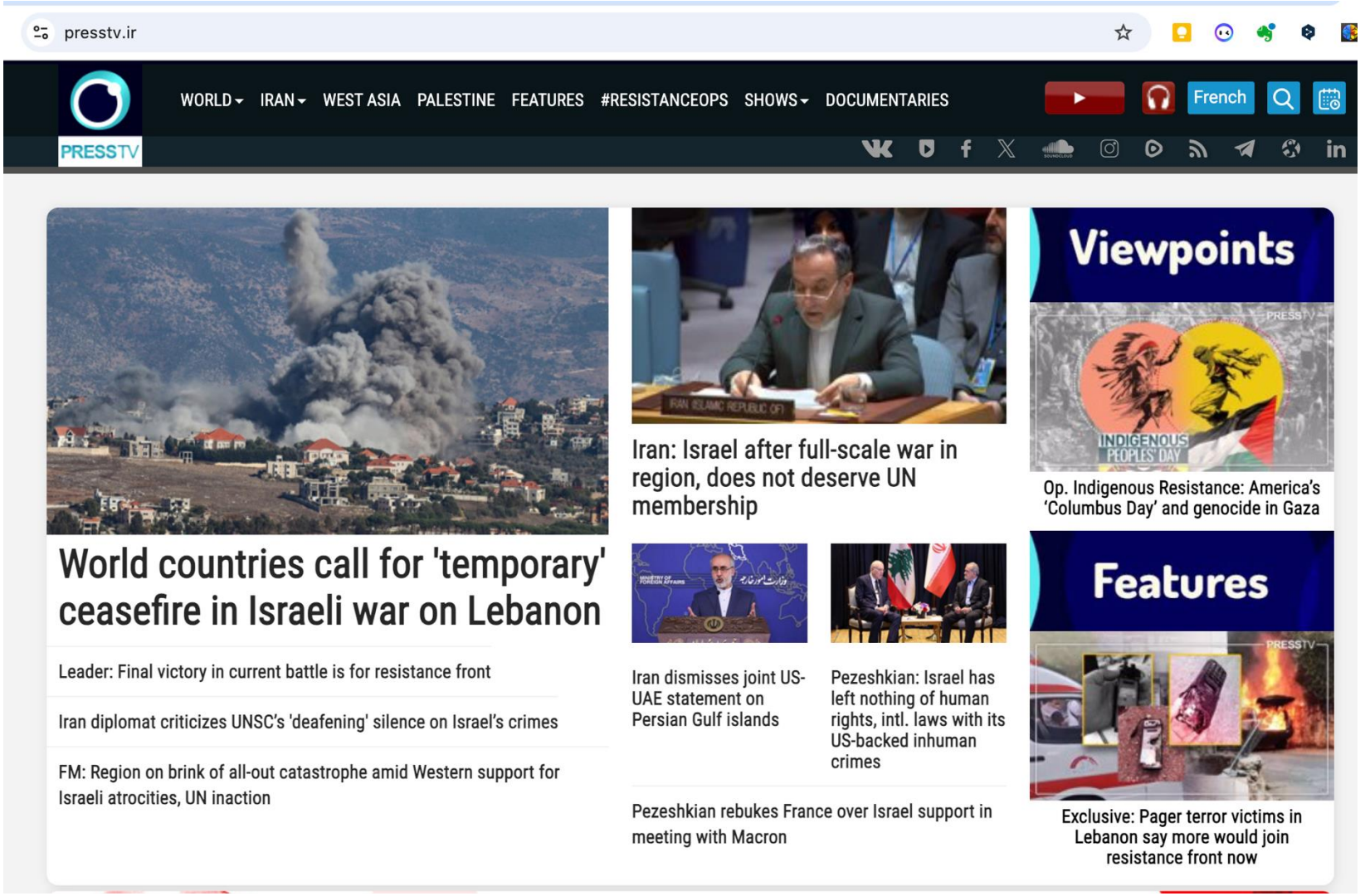
The United States has seized 92 domain names that were unlawfully used by Iran's Islamic Revolutionary Guard Corps (IRGC) to engage in a global disinformation campaign, announced the Department of Justice.

According to the seizure documents, four of the domains purported to be genuine news outlets but were actually controlled by the IRGC and targeted the United States for the spread of Iranian propaganda to influence United States domestic and foreign policy in violation of the Foreign Agents Registration Act (FARA), and the remainder spread Iranian propaganda to other parts of the world. In addition, the seizure documents describe how all 92 domains were being used in violation of U.S. sanctions targeting both the Government of Iran and the IRGC.

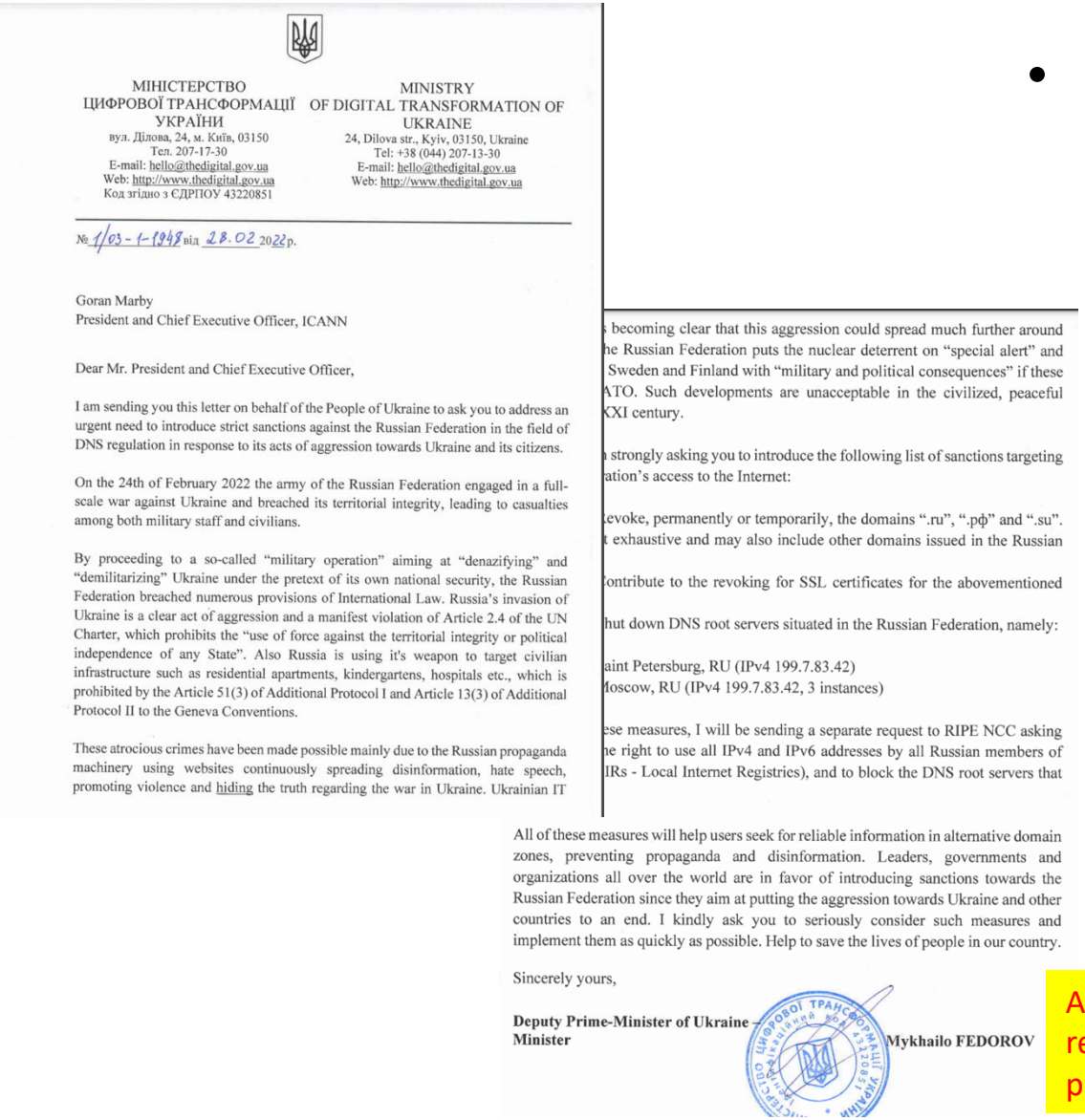
"We will continue to use all of our tools to stop the Iranian Government from misusing U.S. companies and social media to spread propaganda covertly, to attempt to influence the American public secretly, and to sow discord," said Assistant Attorney General for National Security John C. Demers. "Fake news organizations have become a new outlet for disinformation spread by authoritarian countries as they continue to try to undermine our democracy. Today's actions show that we can use a variety of laws to vindicate the value of transparency."

美国司法部公共事务部网站

# 伊朗媒体网站切换IR域名，恢复运营



# 乌总副理呼吁删除俄罗斯顶级域名



МІНІСТЕРСТВО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ
вул. Ділова, 24, м. Київ, 03150
Тел. 207-17-30
E-mail: hello@thedigital.gov.ua
Web: http://www.thedigital.gov.ua
Код згідно з ЄДРПОУ 43220851

MINISTRY OF DIGITAL TRANSFORMATION OF UKRAINE
24, Dilova str., Kyiv, 03150, Ukraine
Tel: +38 (044) 207-13-30
E-mail: hello@thedigital.gov.ua
Web: http://www.thedigital.gov.ua

№ 1/03-1-1948 від 28.02 2022р.

Goran Marby
President and Chief Executive Officer, ICANN

Dear Mr. President and Chief Executive Officer,

I am sending you this letter on behalf of the People of Ukraine to ask you to address an urgent need to introduce strict sanctions against the Russian Federation in the field of DNS regulation in response to its acts of aggression towards Ukraine and its citizens.

On the 24th of February 2022 the army of the Russian Federation engaged in a full-scale war against Ukraine and breached its territorial integrity, leading to casualties among both military staff and civilians.

By proceeding to a so-called "military operation" aiming at "denazifying" and "demilitarizing" Ukraine under the pretext of its own national security, the Russian Federation breached numerous provisions of International Law. Russia's invasion of Ukraine is a clear act of aggression and a manifest violation of Article 2.4 of the UN Charter, which prohibits the "use of force against the territorial integrity or political independence of any State". Also Russia is using it's weapon to target civilian infrastructure such as residential apartments, kindergartens, hospitals etc., which is prohibited by the Article 51(3) of Additional Protocol I and Article 13(3) of Additional Protocol II to the Geneva Conventions.

These atrocious crimes have been made possible mainly due to the Russian propaganda machinery using websites continuously spreading disinformation, hate speech, promoting violence and hiding the truth regarding the war in Ukraine. Ukrainian IT

becoming clear that this aggression could spread much further around
he Russian Federation puts the nuclear deterrent on "special alert" and
Sweden and Finland with "military and political consequences" if these
ATO. Such developments are unacceptable in the civilized, peaceful
XXI century.

strongly asking you to introduce the following list of sanctions targeting
ation's access to the Internet:

evoke, permanently or temporarily, the domains ".ru", ".рф" and ".su".
exhaustive and may also include other domains issued in the Russian

ontribute to the revoking for SSL certificates for the abovementioned

hut down DNS root servers situated in the Russian Federation, namely:

aint Petersburg, RU (IPv4 199.7.83.42)
Moscow, RU (IPv4 199.7.83.42, 3 instances)

ese measures, I will be sending a separate request to RIPE NCC asking
he right to use all IPv4 and IPv6 addresses by all Russian members of
IRs - Local Internet Registries), and to block the DNS root servers that

All of these measures will help users seek for reliable information in alternative domain zones, preventing propaganda and disinformation. Leaders, governments and organizations all over the world are in favor of introducing sanctions towards the Russian Federation since they aim at putting the aggression towards Ukraine and other countries to an end. I kindly ask you to seriously consider such measures and implement them as quickly as possible. Help to save the lives of people in our country.

Sincerely yours,

**Deputy Prime-Minister of Ukraine – Minister** **Mykhailo FEDOROV**

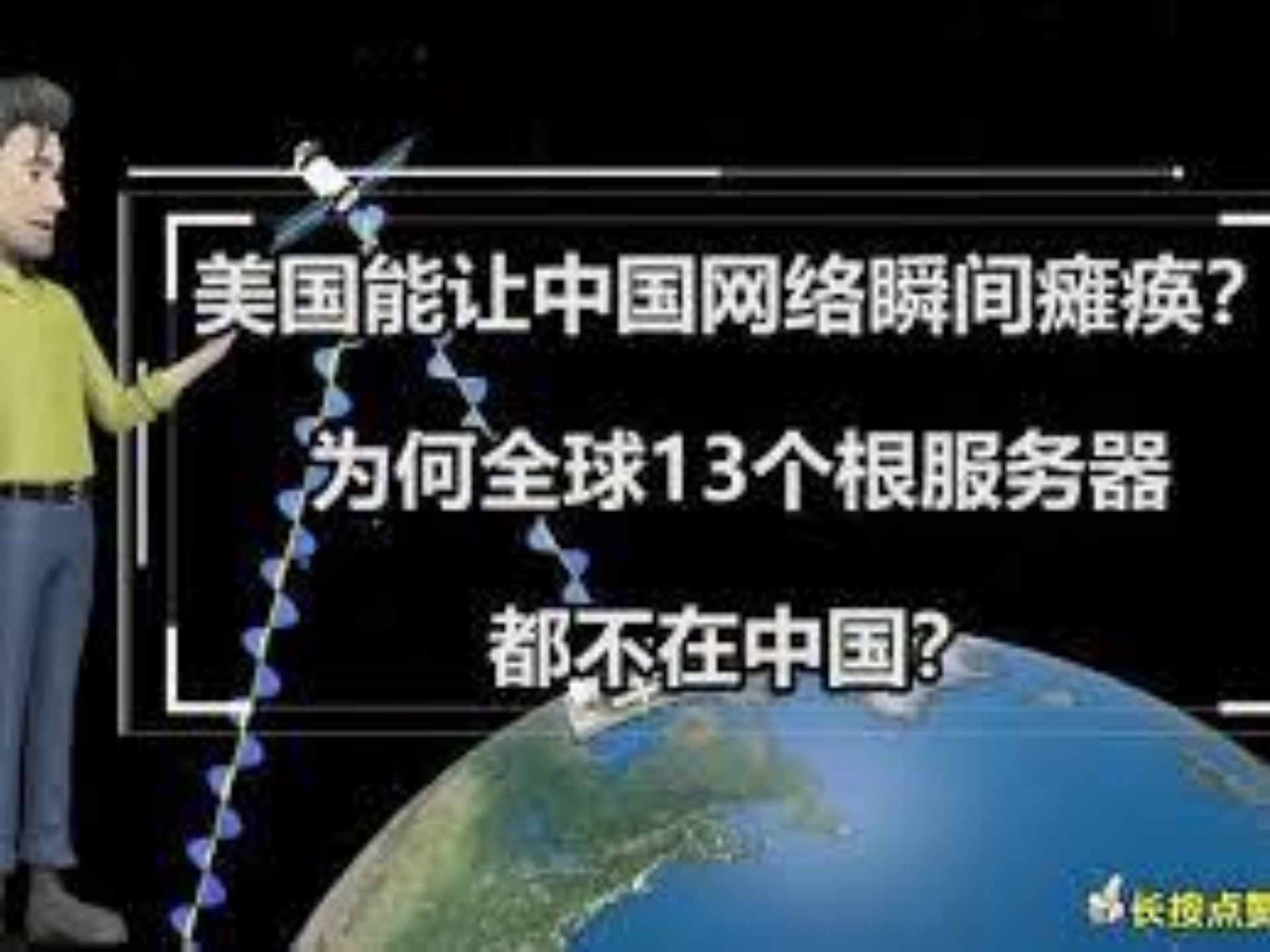
- 乌克兰副总理向ICANN 的诉求：
  - 删除俄罗斯顶级域名
  - 撤销俄罗斯域名下的SSL证书
  - 关掉俄罗斯境内的两个顶级域名
  - 向RIPE NCC 申请撤销IPv4 和IPv6地址

All of these measures will help users seek for reliable information in alternative domain zones, preventing propaganda and disinformation.

《流浪地球2》中重启的北京根域名服务器到底是什么来头

3420 101 2023-02-03 21:18:29


《流浪地球2》中重启的北京根域名服务器到底是什么来头
https://www.bilibili.com/video/BV1gY411q7qW


美国能让中国网络瞬间瘫痪?
为何全球13个根服务器
都不在中国?

# 大學該教什麼？ 哈佛校長開學致辭：能分辨有人在胡說八道

2017-10-17 16:11 聯合報 / 好讀周報



好萊塢名導史帝芬史匹柏（圖左）及臉書創辦人祖克柏，都曾應邀在哈佛畢業典禮上致詞，圖右即哈佛校長福斯特。路透、美聯社

# 为什么关注DNS安全？

- DNS是互联网的基础服务，常常成为大规模攻击的目标，可使大范围的网络瘫痪
- DNS是多种网络安全机制的基础，如电子邮件、公钥证书、Web 和CDN等
- DNS流量是防火墙等安全设备允许的，也常作为攻击的工具、隐蔽信道，难以过滤和防范
- 域名常被滥用，成为钓鱼、诈骗等攻击的工具
- DNS 治理一直是国际关系中互联网治理的焦点

# 目录

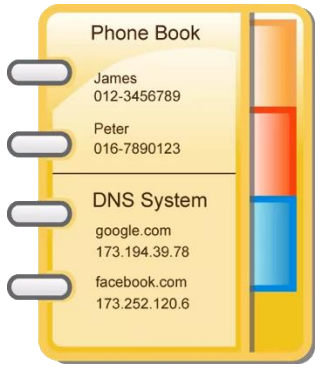
- DNS 攻击事件
- DNS 服务的功能
- DNS 系统和工作原理
- DNS 协议格式
- DNS 攻击面

# DNS 服务的功能

- 名字和地址的映射： Name <- -> IP
- 邮件路由 MX
- Web内容路由: CDN
- 邮件信任的基础: SPF
- 证书申请的信任基础

# Mapping: Domain name←→IP

- Name -> IP ;  IP→ Name?

www.tsinghua.edu.cn → 

→ 166.111.4.100

166.111.4.100 →  → www.tsinghua.edu.cn

```
% dig www.tsinghua.edu.cn

;; QUESTION SECTION:
;www.tsinghua.edu.cn.        IN      A

;; ANSWER SECTION:
www.tsinghua.edu.cn.  21103 IN  A 166.111.4.100

;; Query time: 1 msec
```

```
% dig -x 166.111.4.100

;; QUESTION SECTION:
;100.4.111.166.in-addr.arpa.        IN      PTR

;; ANSWER SECTION:
100.4.111.166.in-addr.arpa. 86161 IN PTR www.tsinghua.

;; Query time: 8 msec
```

# DNS Tool: dig

- dig -t <type> @resolver <name> +<flags>
  - Type:
    - A: Address,
    - AAAA: IPv6 Address
    - CNAME: Alias ,
    - NS: Name Server,
    - TXT: text
    - SOA : start of Authority
    - PTR: reverse pointer to IP
- Options:
  - +trace, +tcp, +norecursive, +dnssec,…
- E.g.
  - dig @166.111.8.28 -t ns mit.edu +tcp

Linux, Mac 自带，Windows 用户下载安装：https://www.isc.org/download/

# DNS 资源记录
# （Resource Record）

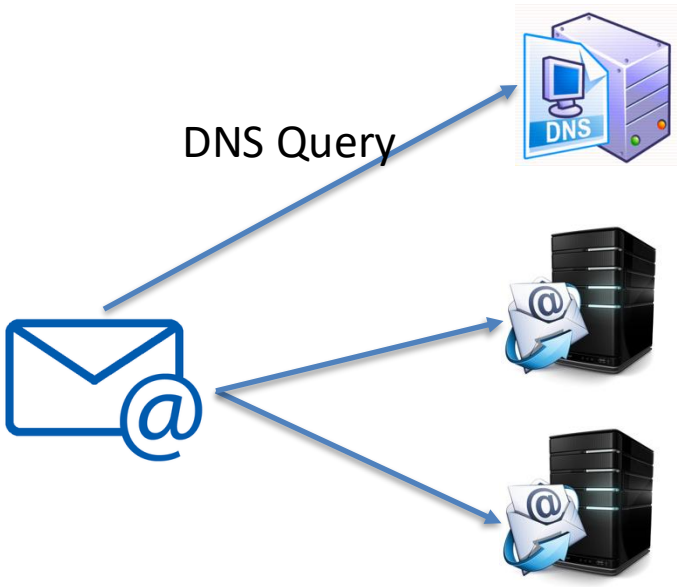
| Type | Description |
|---|---|
| A | IP Address |
| AAAA | IPv6 Address |
| CNAME | Canonical name record |
| MX | Mail exchange record |
| PTR | Pointer |
| SOA | Start of [a zone of] authority record |
| TLSA | TLSA certificate association |
| TXT | Text record, opportunistic encryption, Sender Policy Framework, DKIM, DMARC, DNS-SD, etc. |
| * | All cached records |
| AXFR | Authoritative Zone Transfer |
| OPT | pseudo DNS record type needed to support EDNS |

```
duanhx@HaixindeiMac-Pro ~ % dig any tsinghua.edu.cn

; <<>> DiG 9.10.6 <<>> any tsinghua.edu.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41554
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 11

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;tsinghua.edu.cn.               IN      ANY

;; ANSWER SECTION:
tsinghua.edu.cn.        44059   IN      NS      dns.edu.cn.
tsinghua.edu.cn.        44059   IN      NS      dns2.tsinghua.edu.cn.
tsinghua.edu.cn.        44059   IN      NS      dns2.edu.cn.
tsinghua.edu.cn.        44059   IN      NS      dns.tsinghua.edu.cn.
tsinghua.edu.cn.        34857   IN      MX      10 mta1.tsinghua.edu.cn.
tsinghua.edu.cn.        34857   IN      MX      10 mta0.tsinghua.edu.cn.

;; ADDITIONAL SECTION:
dns.edu.cn.             119651  IN      A       202.38.109.35
dns.tsinghua.edu.cn.    44060   IN      A       166.111.8.30
dns2.edu.cn.            119651  IN      A       202.112.0.13
dns2.tsinghua.edu.cn.   44060   IN      A       166.111.8.31
mta0.tsinghua.edu.cn.   34857   IN      A       166.111.204.8
mta1.tsinghua.edu.cn.   34857   IN      A       166.111.204.9
dns.edu.cn.             119651  IN      AAAA    2001:250:c006::35
dns.tsinghua.edu.cn.    44060   IN      AAAA    2402:f000:1:801::8:30
dns2.edu.cn.            119652  IN      AAAA    2001:da8:1:100::13
dns2.tsinghua.edu.cn.   44060   IN      AAAA    2402:f000:1:801::8:31
```

```
duanhx@MBP-abai ~ % dig  twitter.com @a.r06.twtrdns.net. any +dnssec
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.10.6 <<>> twitter.com @a.r06.twtrdns.net. any +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11319
;; flags: qr aa rd ad; QUERY: 1, ANSWER: 27, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;twitter.com.                   IN      ANY

;; ANSWER SECTION:
twitter.com.            1800    IN      A       104.244.42.1
twitter.com.            13999   IN      NS      a.r06.twtrdns.net.
twitter.com.            13999   IN      NS      b.r06.twtrdns.net.
twitter.com.            13999   IN      NS      c.r06.twtrdns.net.
twitter.com.            13999   IN      NS      d.r06.twtrdns.net.
twitter.com.            13999   IN      NS      d01-01.ns.twtrdns.net.
twitter.com.            13999   IN      NS      d01-02.ns.twtrdns.net.
twitter.com.            13999   IN      NS      ns1.p34.dynect.net.
twitter.com.            13999   IN      NS      ns2.p34.dynect.net.
twitter.com.            13999   IN      NS      ns3.p34.dynect.net.
twitter.com.            13999   IN      NS      ns4.p34.dynect.net.
twitter.com.            293     IN      SOA     ns1.p26.dynect.net. zone-admin.dyndns.com. 2007176347 3600 600 604800 60
twitter.com.            600     IN      MX      10 aspmx.l.google.com.
twitter.com.            600     IN      MX      20 alt1.aspmx.l.google.com.
twitter.com.            600     IN      MX      20 alt2.aspmx.l.google.com.
twitter.com.            600     IN      MX      30 aspmx2.googlemail.com.
twitter.com.            600     IN      MX      30 aspmx3.googlemail.com.
twitter.com.            3600    IN      TXT     "MS=BEE202D20C326867290BDEFA2DDDF4594B5D6860"
twitter.com.            3600    IN      TXT     "adobe-idp-site-verification=a2ff8fc40c434d1d6f02f68b0b1a683e400572ab8c1f2c180c71c3d985b9270a"
twitter.com.            3600    IN      TXT     "apple-domain-verification=zd1iHoEO9LILEQIq"
twitter.com.            3600    IN      TXT     "atlassian-domain-verification=CCYSIJhsAnbjYWrbdw5r//aHNsYnzgv7Z6Gwz4TkAv5OYdZt3Lm/ycLxT2tmfm/n"
twitter.com.            3600    IN      TXT     "canva-site-verification=lMnZ3wMh7c1uqZqa-cxZTg"
twitter.com.            3600    IN      TXT     "google-site-verification=TNhAkfLUeIbzzzSgPNxS5aEkKMf3aUcpPmCK1_kmIvU"
twitter.com.            3600    IN      TXT     "google-site-verification=h6dJIv0HXjLOkGAotLAWEzvoi9SxqP4vjpx98vrCvvQ"
twitter.com.            3600    IN      TXT     "loom-site-verification=638c6bc173b9458997f64d305bf42499"
twitter.com.            3600    IN      TXT     "traction-guest=6882b04e-4188-4ff9-8bb4-bff5a3d358e6"
twitter.com.            3600    IN      TXT     "v=spf1 ip4:199.16.156.0/22 ip4:199.59.148.0/22 ip4:8.25.194.0/23 ip4:8.25.196.0/23 ip4:204.92.114.
203 ip4:204.92.114.204/31 ip4:54.156.255.69 include:_spf.google.com include:_thirdparty.twitter.com include:spf.smtp2go.com -all"
```

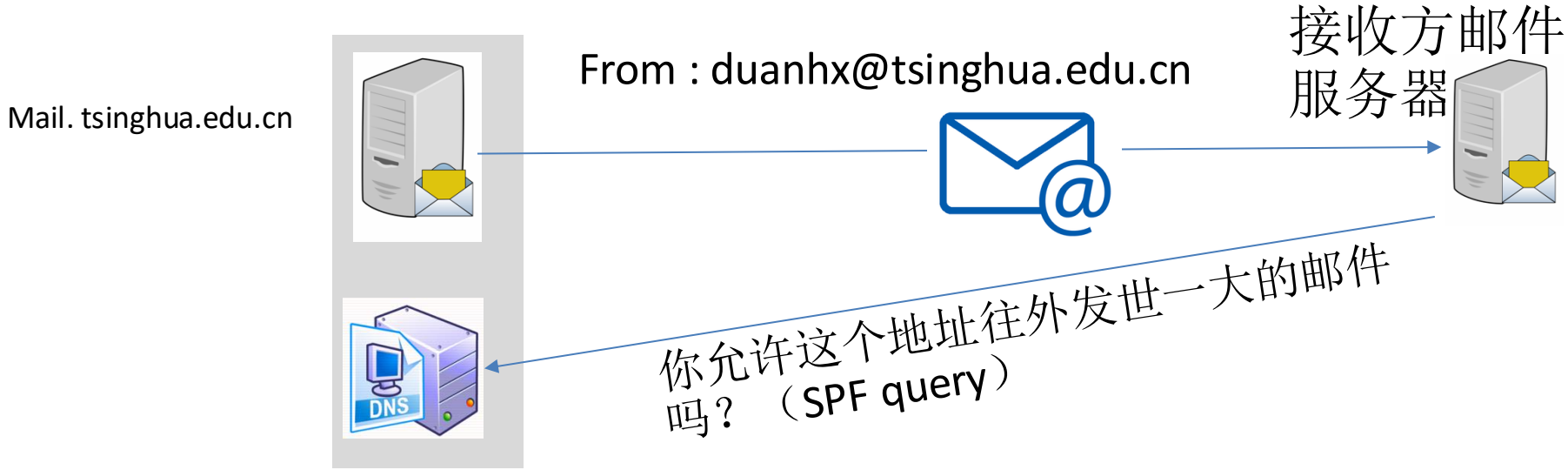
# 邮件路由

- DNS 中的 MX记录 mailto: duanhx@tsinghua.edu.cn




```
% dig mx tsinghua.edu.cn

;; ANSWER SECTION:
tsinghua.edu.cn.  21600   IN   MX   10 mta0.tsinghua.edu.cn.
tsinghua.edu.cn.  21600   IN   MX   10 mta1.tsinghua.edu.cn.

;; ADDITIONAL SECTION:
mta0.tsinghua.edu.cn.     7200 IN   A    166.111.204.8
mta1.tsinghua.edu.cn.     7200 IN   A    166.111.204.9
```

# DNS作为信任的基础支持邮件服务器的验证




```
bash-3.2# dig -t txt spf.tsinghua.edu.cn

; <<>> DiG 9.12.3-P1 <<>> -t txt spf.tsinghua.edu.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7939
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;spf.tsinghua.edu.cn.           IN      TXT

;; ANSWER SECTION:
spf.tsinghua.edu.cn.    21575   IN      TXT     "v=spf1 ip4:101.6.4.0/24 ip4:166.111.204.0/24 ip4:166
.111.2.24/29 ip4:59.66.3.24/29 ip4:101.5.3.24/29 ip4:101.6.3.24/29 ip4:183.172.3.24/29 ip4:183.173.3.
24/29 include:spf.icoremail.net ~all"
```

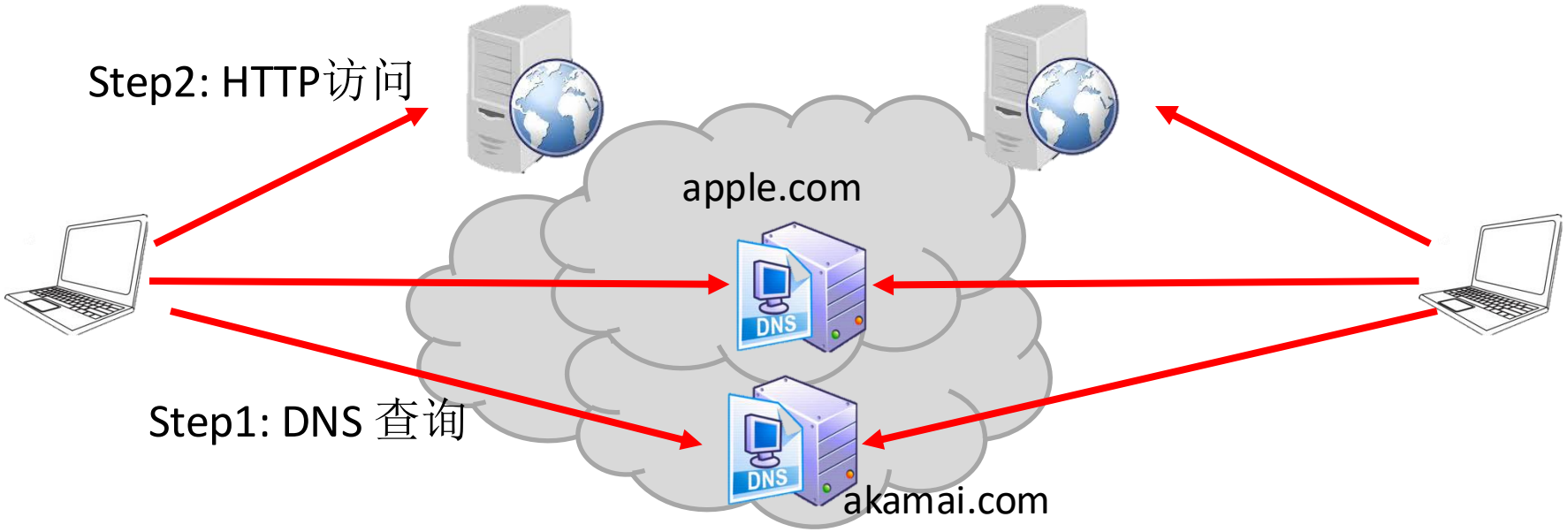
# TXT 资源记录与 SPF记录

```
duanhx@HaixindeiMac-Pro ~ % dig txt tsinghua.edu.cn

; <<>> DiG 9.10.6 <<>> txt tsinghua.edu.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47001
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;tsinghua.edu.cn.               IN      TXT

;; ANSWER SECTION:
tsinghua.edu.cn.        86348   IN      TXT     "adobe-idp-site-verification=3e2296d0c59d5fda8f42086830f3c085e951b94ec9302e74b41637e3311481d9"
tsinghua.edu.cn.        86348   IN      TXT     "v=spf1 redirect=spf.tsinghua.edu.cn"
```

```
duanhx@HaixindeiMac-Pro ~ % dig txt spf.tsinghua.edu.cn

; <<>> DiG 9.10.6 <<>> txt spf.tsinghua.edu.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42801
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;spf.tsinghua.edu.cn.           IN      TXT

;; ANSWER SECTION:
spf.tsinghua.edu.cn.    7190    IN      TXT     "v=spf1 ip4:101.6.4.0/24 ip4:166.111.204.0/24 ip4:166.111.2.24/29 ip4:59.66.3.24/29 ip4:101.5.3.24/29 ip4:101.6.3.24/29
ip4:183.172.3.24/29 ip4:183.173.3.24/29 include:spf.icoremail.net -all"
```

```
;; ANSWER SECTION:
spf1.icoremail.net.     180     IN      TXT     "v=spf1 ip4:223.252.214.0/24 ip4:119.147.163.192/27 ip4:157.255.37.64/27 ip4:106.2.96.0/24 ip4:59.111.192.0/23 ip4:115.2
36.118.128/26 ip4:101.71.145.0/26 ip4:112.13.121.64/26 a:jdcloud-cloud.icoremail.net ~all"
```

# CDN基于DNS提供内容分发和负载均衡




```
duanhx@HaixindeiMac-Pro ~ % dig  www.apple.com

; <<>> DiG 9.10.6 <<>> www.apple.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50254
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.apple.com.                 IN      A

;; ANSWER SECTION:
www.apple.com.          574     IN      CNAME   www.apple.com.edgekey.net.
www.apple.com.edgekey.net. 18592 IN     CNAME   www.apple.com.edgekey.net.globalredir.akadns.net.
www.apple.com.edgekey.net.globalredir.akadns.net. 2344 IN CNAME e6858.e19.s.tl88.net.
e6858.e19.s.tl88.net.   494     IN      A       23.196.120.215
```

```
duanhx@HaixindeiMac-Pro ~ % dig  www.apple.com @8.8.8.8

; <<>> DiG 9.10.6 <<>> www.apple.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31534
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.apple.com.                 IN      A

;; ANSWER SECTION:
www.apple.com.          1642    IN      CNAME   www.apple.com.edgekey.net.
www.apple.com.edgekey.net. 15240 IN     CNAME   www.apple.com.edgekey.net.globalredir.akadns.n
www.apple.com.edgekey.net.globalredir.akadns.net. 3600 IN CNAME e6858.dscx.akamaiedge.net.
e6858.dscx.akamaiedge.net. 18   IN      A       23.44.52.254
```

# DNS作为信任基础支持公钥证书申请

www.MyDomain.com

1. 申请证书for www.MyDomain.com

CA
GlobalSign


2. 你能把这个随机生成的字符串放到你的DNS权威服务器上，我就相信你拥有MyDomain.com

NS.MyDomain.com


DNS query: TXT _globalsign-www.mydomain.com-verification

DNS TXT Record:

DNS TXT Record: _globalsign-domain-verification=WONkt7Og6t_p0WhGT9pHasZU8AN7oS4XvzYqZeBOu-

# DNS作为信任的根基

- 网站口令恢复➔ 发邮件➔ 依赖DNS

- DNS不安全，域名不可信➔向CA申请公钥证书➔ CA依赖DNS来确认网站的身份

# RFC8567:用DNS存密码/信用卡/SSN

https://tools.ietf.org/html/rfc8567

[Docs] [txt|pdf] [draft-ietf-cust...] [Tracker] [Diff1] [Diff2]

INFORMATIONAL

Independent Submission — E. Rye
Request for Comments: 8567 — R. Beverly
Category: Informational — CMAND
ISSN: 2070-1721 — 1 April 2019

**Customer Management DNS Resource Records**


Abstract

Maintaining high Quality of Experience (QoE) increasingly requires end-to-end, holistic network management, including managed Customer Premises Equipment (CPE). Because customer management is a shared global responsibility, the Domain Name System (DNS) provides an ideal existing infrastructure for maintaining authoritative customer information that must be readily, reliably, and publicly accessible.

This document describes four new DNS resource record types for encoding customer information in the DNS. These records are intended to better facilitate high customer QoE via inter-provider cooperation and management of customer data.


https://tools.ietf.org/html/rfc8567

Table of Contents



## 1. Introduction

A significant portion of today's Internet is comprised of residential access networks. These access networks, and their providers, are now critical infrastructure, and significant research is devoted to measuring residential broadband speed and reliability [SAMKNOWS].

Unfortunately, Customer Premises Equipment (CPE) is one of the weakest links in the chain of network equipment connecting consumers to the Internet. Customers typically do not perform proactive maintenance, e.g., firmware updates, on their own CPE. In many cases, CPE is even deployed with default authentication credentials, a fact that has been exploited by various Internet-wide denial-of-service attacks [MIRAI].

## 2.1. The PASSWORD Resource Record

The PASSWORD RR facilitates remote management of CPE devices by providing the login credentials for the CPE in a single RR. Thes credentials are used by authorized service providers to authentic to the CPE. Authenticated users can then install important softw and configuration updates to benefit the security and health of t provider's network.

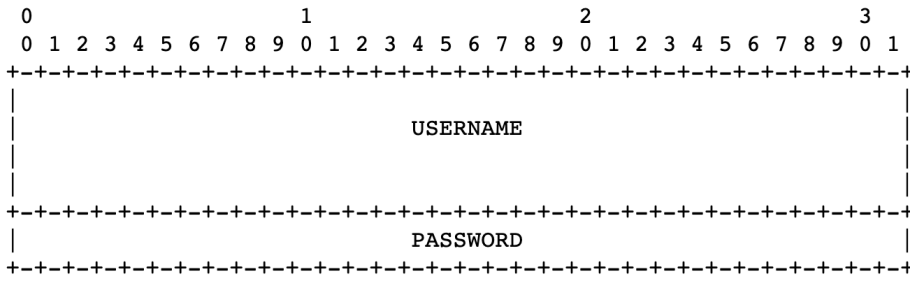



Figure 1: PASSWORD RDATA Format

Where:

USERNAME
The <character-string> username of the account holder located the CPE. In order to limit gratuitous expressions of individuality, usernames MUST be 16 or fewer ASCII characters MUST NOT include punctuation.

PASSWORD
The <character-string> password associated with the USERNAME. order to keep the RR size to a minimum, passwords longer than bits are NOT supported.

Hosts on which multiple accounts exist SHOULD have separate PASSW RRs for each account.

## 2.2. The CREDITCARD Resource Record

The CREDITCARD RR stores the billing details of the primary account holder located at the hostname associated with the CPE. Upon gaining a new subscriber, an ISP enters their billing details in a CREDITCARD RR so that it MAY be queried as needed for automated billing purposes. In addition, any outside entity with whom the customer





develops a recurring payment plan MAY query this RR for payment details as well. Storing payment information in an RR, rather than in the databases of disparate organizations with varying data security postures, helps reduce attack vectors available to malicious actors seeking this data.

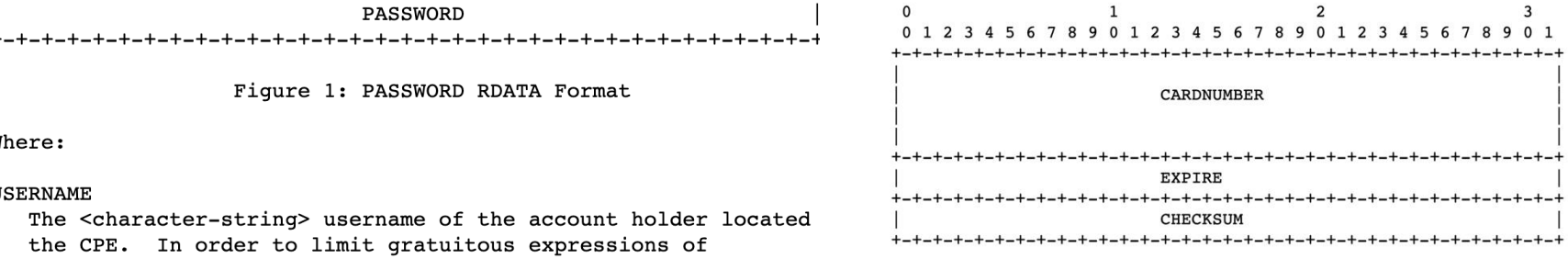



Figure 2: CREDITCARD RDATA Format

Where:

CARDNUMBER
The <character-string> 16-digit credit card number used for billing by the host's service provider. This field MUST NOT contain punctuation or spaces; only numeric digits represented in ASCII are allowed. Because this field is 16 digits in length, users MUST NOT use American Express cards.

EXPIRE

INFORMATIONAL

Independent Submission
Request for Comments: 8567
Category: Informational
ISSN: 2070-1721

E. Rye
R. Beverly
CMAND

1 April 2019

# Customer Management DNS Resource Records

## Abstract

Maintaining high Quality of Experience (QoE) increasingly requires end-to-end, holistic network management, including managed Customer Premises Equipment (CPE). Because customer management is a shared global responsibility, the Domain Name System (DNS) provides an ideal existing infrastructure for maintaining authoritative customer information that must be readily, reliably, and publicly accessible.

This document describes four new DNS resource record types for encoding customer information in the DNS. These records are intended to better facilitate high customer QoE via inter-provider cooperation and management of customer data.

# 目录

- DNS 攻击事件
- DNS 服务的功能
- DNS 系统和工作原理
- DNS 协议格式
- DNS 的根Root及其管理

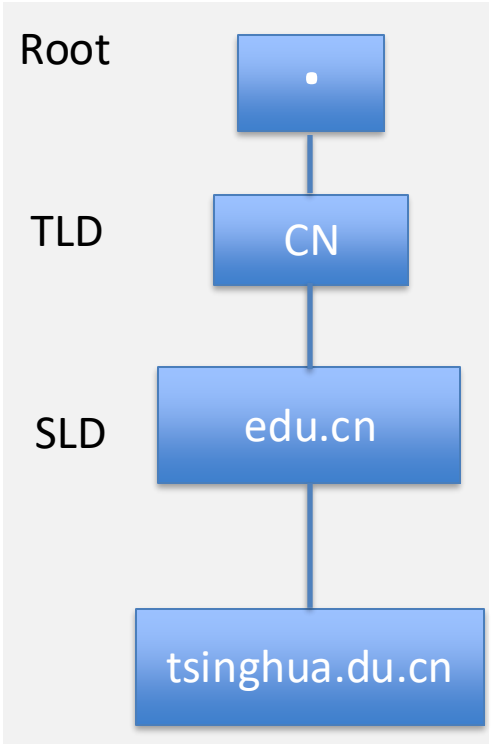
# Pre-DNS: HOSTS.txt

- Before DNS(1983):
  - /etc/hosts,

```
duanhx@HaixindeiMac-Pro ~ % more /etc/hosts
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting.  Do not change this entry.
##
127.0.0.1       localhost
255.255.255.255 broadcasthost
::1             localhost
# Added by Docker Desktop
# To allow the same kube context to work on the host and the container:
127.0.0.1 kubernetes.docker.internal
# End of section
```

- Windows NT/2000/XP/2003/Vista:
  - %SystemRoot%\system32\drivers\etc\hosts
  - \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DataBasePath
- Lookup: Hosts first, then DNS, …
- Bypass DNS by Hosts….
  - Hacker …
  - The Big Brother … https://code.google.com/p/smarthosts/

# 问题：假设所有的缓存都是空的，请问DNS查询的过程?




Nameserver
(166.111.8.28)

www.tsinghua.edu.cn

Desktop

www.tsinghua.edu.cn

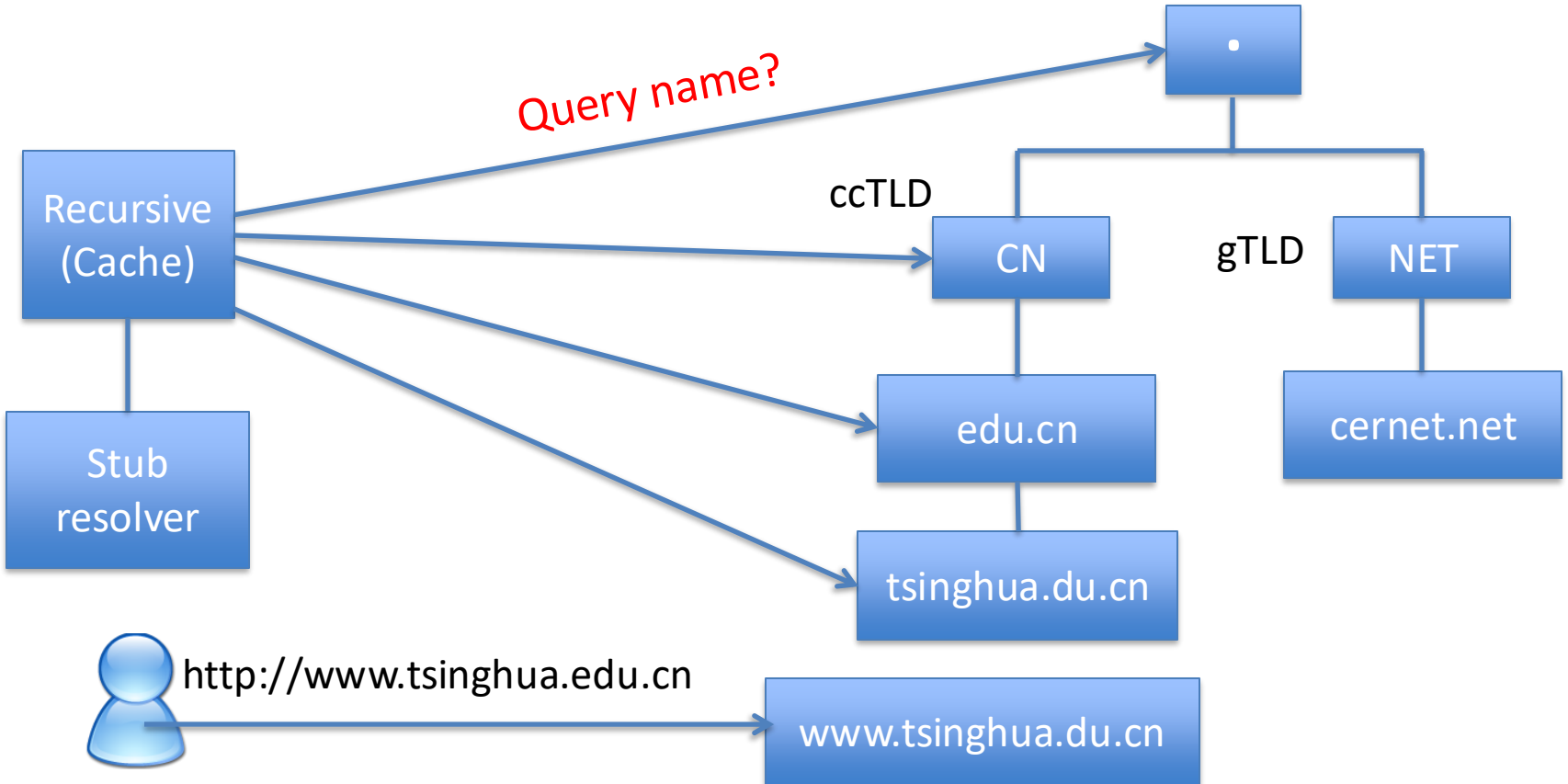
http://www.tsinghua.edu.cn

# DNS查询工作过程

客户端：递归/缓存
- Cache, Recursive

UDP/TCP

权威服务器（Authoritative）
Root, TLD, SLD…



# 三种查询方式

- 递归查询
  - dig [+rec] @8.8.8.8 edu.cn
  - 要求目标服务器把最终的结果返回，如果查不到最终结果，则返回错误
- 非递归查询
  - dig +norec @8.8.8.8 www.edu.cn
  - 要求目标服务器返回缓存里的结果（如果有），不去递归
- 迭代查询
  - dig +trace www.edu.cn
  - 自己从根开始依次执行非递归查询，直至得到最终结果，或者失败

```
[duanhx@mm1213 ~]$ dig +trace www.tsinghua.edu.cn

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> +trace www.tsinghua.edu.cn
;; global options: +cmd
.                       251628  IN      NS      b.root-servers.net.
.                       251628  IN      NS      g.root-servers.net.
.                       251628  IN      NS      j.root-servers.net.
.                       251628  IN      NS      a.root-servers.net.
.                       251628  IN      NS      l.root-servers.net.
.                       251628  IN      NS      f.root-servers.net.
.                       251628  IN      NS      c.root-servers.net.
.                       251628  IN      NS      m.root-servers.net.
.                       251628  IN      NS      k.root-servers.net.
.                       251628  IN      NS      e.root-servers.net.
.                       251628  IN      NS      d.root-servers.net.
.                       251628  IN      NS      i.root-servers.net.
.                       251628  IN      NS      h.root-servers.net.
;; Received 508 bytes from 166.111.133.223#53(166.111.133.223) in 2476 ms

cn.                     172800  IN      NS      d.dns.cn.
cn.                     172800  IN      NS      b.dns.cn.
cn.                     172800  IN      NS      e.dns.cn.
cn.                     172800  IN      NS      ns.cernet.net.
cn.                     172800  IN      NS      a.dns.cn.
cn.                     172800  IN      NS      c.dns.cn.
;; Received 300 bytes from 192.228.79.201#53(192.228.79.201) in 253 ms

edu.cn.                 172800  IN      NS      ns2.cernet.net.
edu.cn.                 172800  IN      NS      dns.edu.cn.
edu.cn.                 172800  IN      NS      deneb.dfn.de.
edu.cn.                 172800  IN      NS      ns2.cuhk.hk.
edu.cn.                 172800  IN      NS      dns2.edu.cn.
;; Received 185 bytes from 203.119.27.1#53(203.119.27.1) in 958 ms

www.tsinghua.edu.cn.    21600   IN      CNAME   www.d.tsinghua.edu.cn.
d.tsinghua.edu.cn.      21600   IN      NS      dns.d.tsinghua.edu.cn.
;; Received 107 bytes from 137.189.6.21#53(137.189.6.21) in 313 ms
```

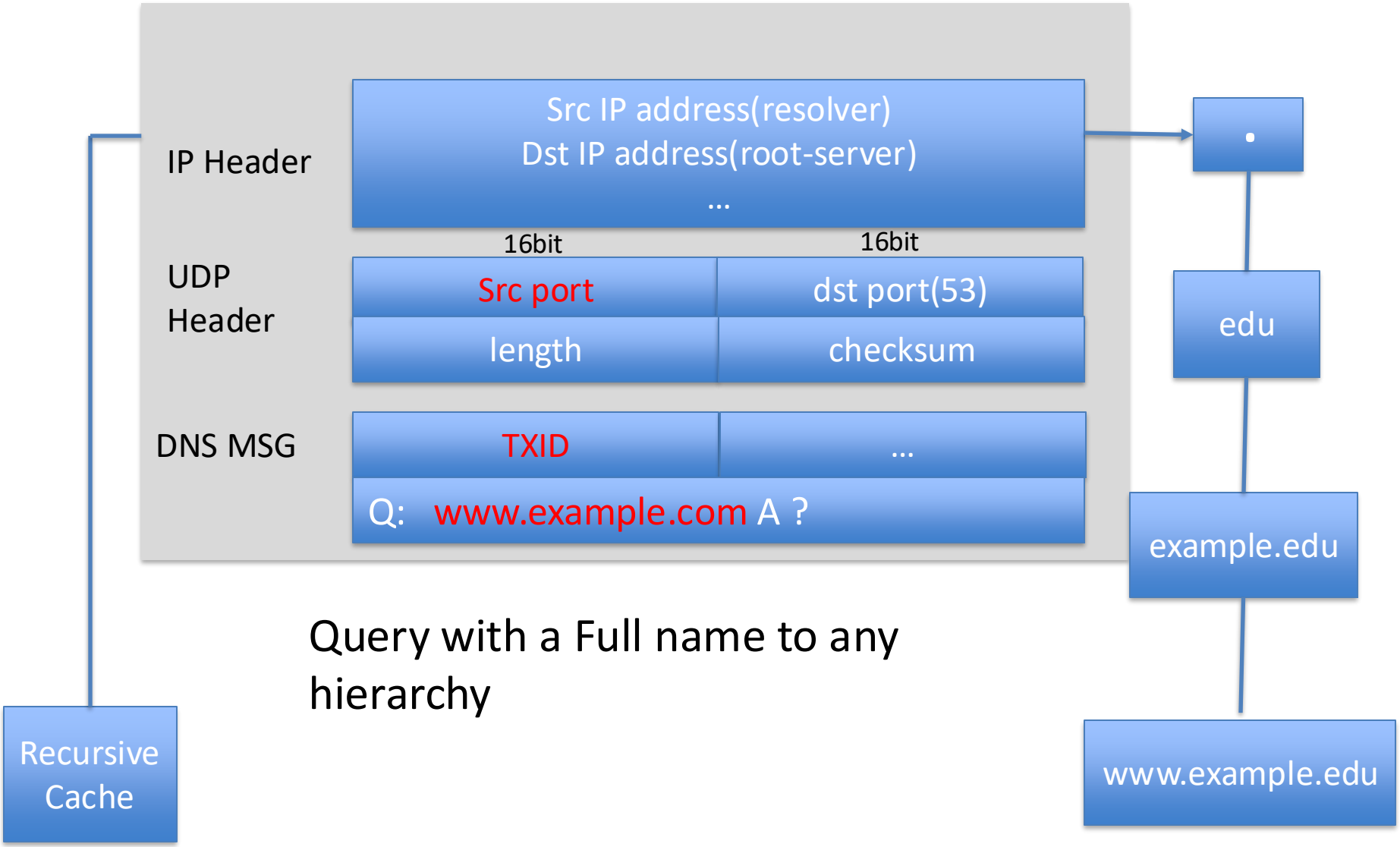
b.root-servers.net.

c.dns.cn.

ns2.cuhk.hk.

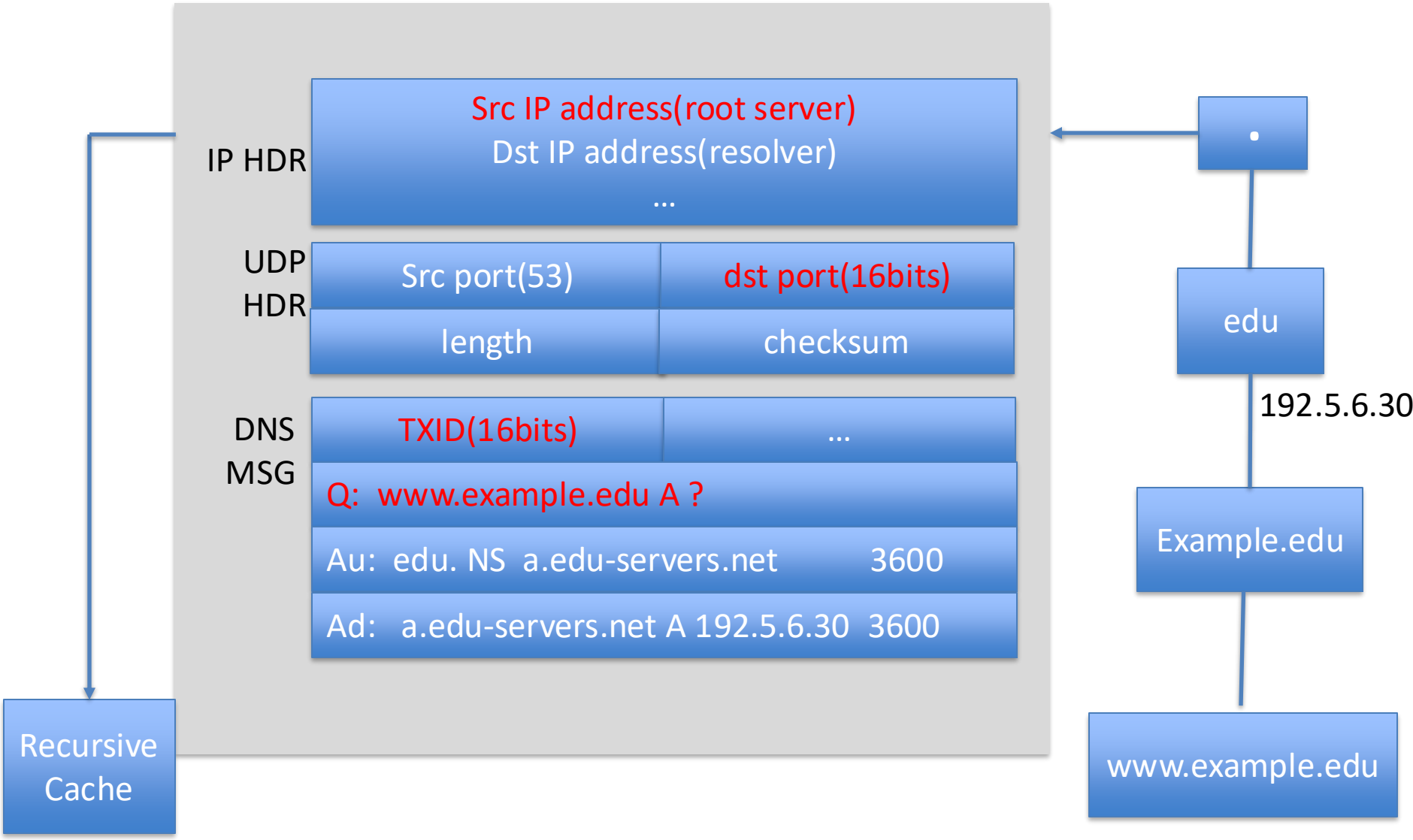
```
bind.keys  db.0  db.127  db.255  db.empty  db.local  db.root  named.conf  named.conf.default-zo
root@haixin-VirtualBox:/etc/bind# more db.root
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    February 17, 2016
;       related version of root zone:   2016021701
;
; formerly NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:84::b
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
C.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     199.7.91.13
D.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
```

# DNS Request

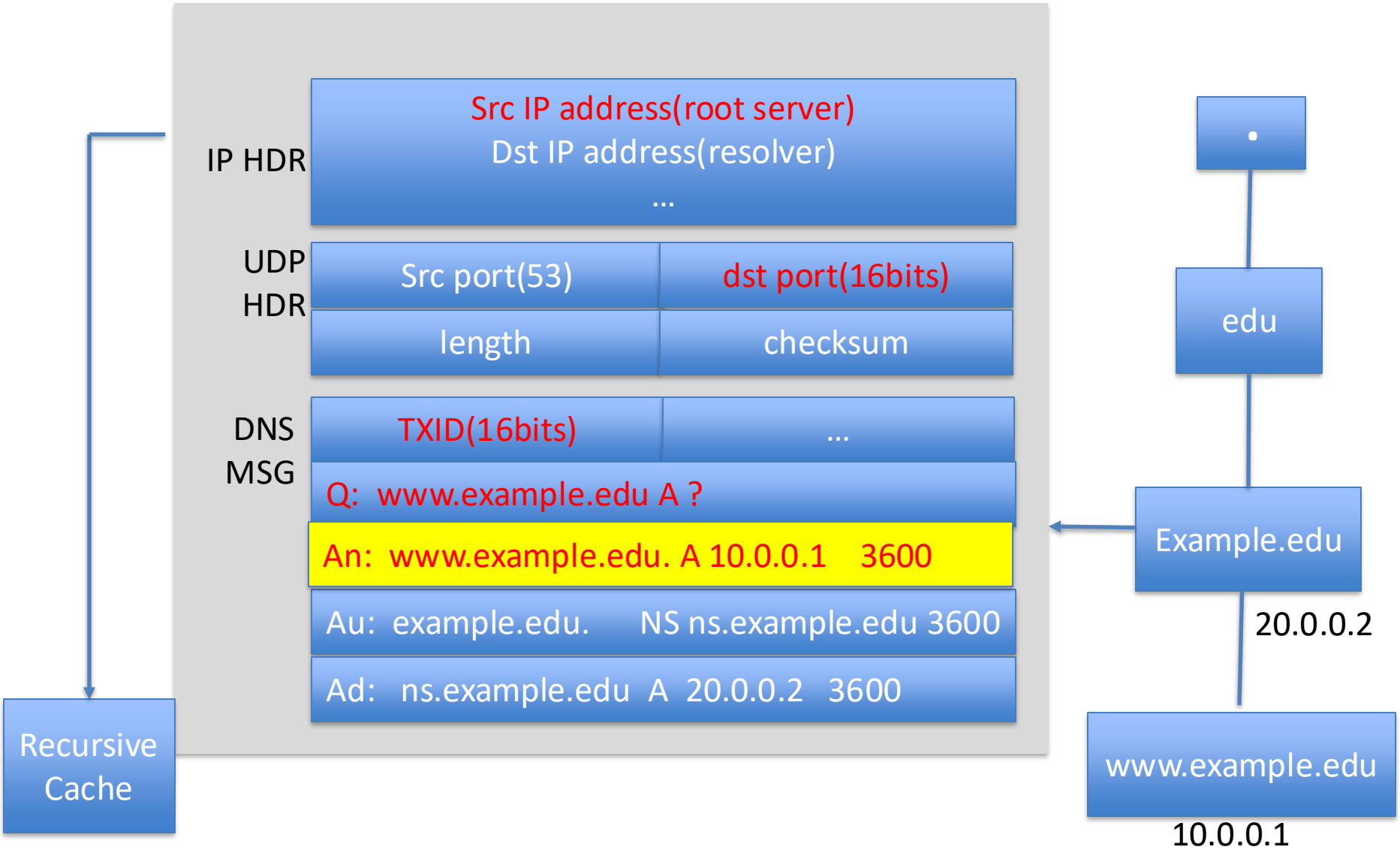



Query with a Full name to any hierarchy

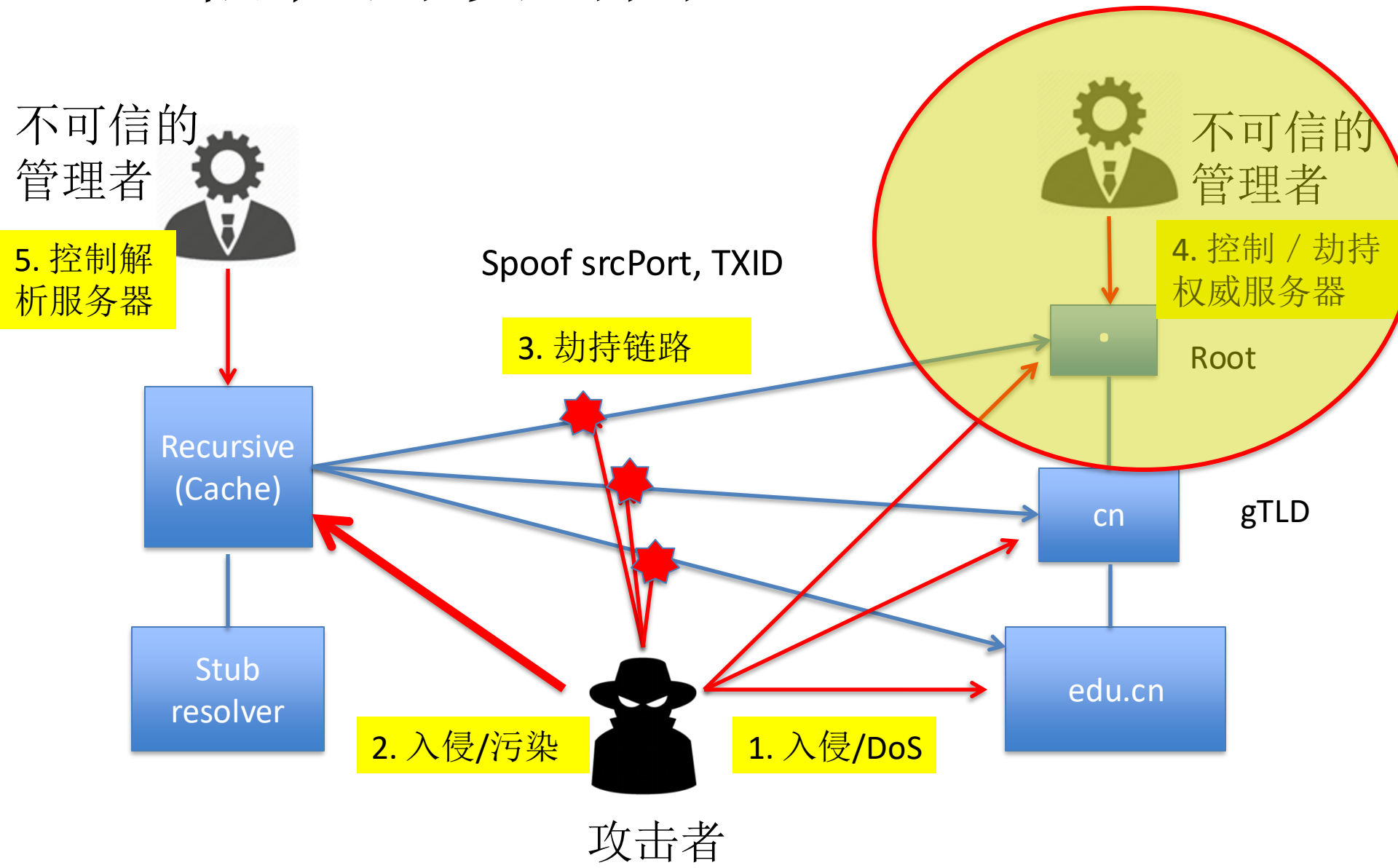
# DNS Reply from Root



# DNS reply from Authoritative Server

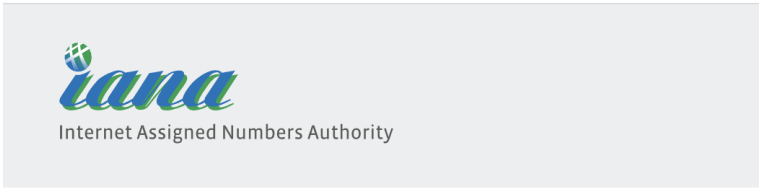


# DNS信任的攻击面（attack surface）



# 对DNS Root 的攻击及威胁

- 13个根，编号 A-M,
  - 为什么是13？
- 篡改根中的数据
  - TLD Zone File




Domain Names

Overview
**Root Zone Management**
Overview
Root Database
**Hint and Zone Files**
Change Requests
Instructions & Guides
Root Servers
.INT Registry
.ARPA Registry
IDN Practices Repository
Root Key Signing Key (DNSSEC)
Reserved Domains

## Root Files

### Root Hints

Operators who manage a DNS recursi
addresses of the authoritative name s
of software, this list comes built into th

- Root Hints File (FTP)
- Root Hints File (HTTP)

### Root Zone File

The complete root zone is available fo
regular basis, as the contents of the fil

- Root Zone File (FTP)
- Root Zone File (HTTP)

### Root Trust Anchor

The Root Trust Anchor, or *Key Signing K*
additionally enables a single chain of t

- Root Trust Anchors

### Top-Level Domains

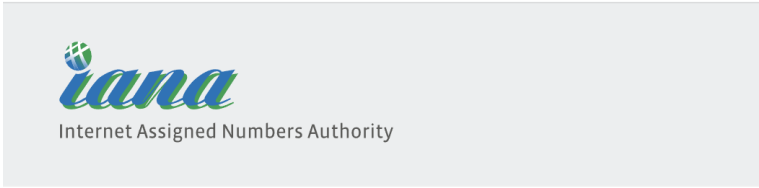
A plain-text list of top-level domains, th
of current top-level domains.

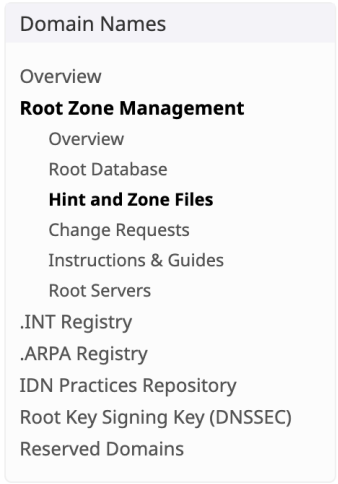
- Top-Level Domain List

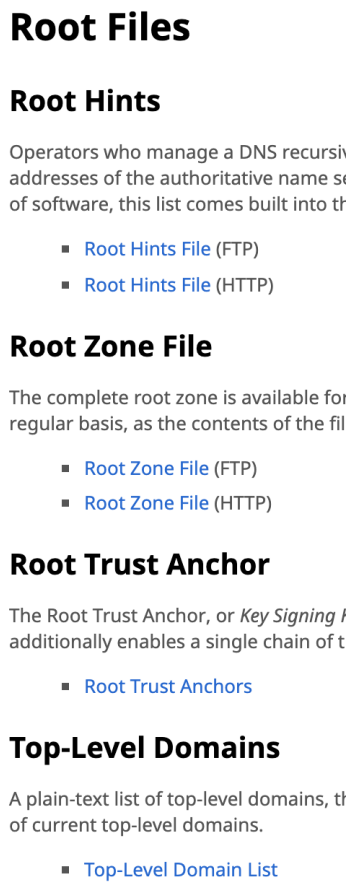
https://www.iana.org/domains/root/files

# 对DNS Root 的攻击及威胁

- 13个根，编号 A-M,
  - 为什么是13？
- 篡改根中的数据
  - TLD Zone File
- 拒绝服务攻击




https://www.iana.org/domains/root/files

# DNS早期的历史

- 1970+，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（1984）
- 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），收费注册
- 互联网在全球迅速发展，欧洲、日本部署了两个根
- 1987年 RFC 1035，限制 DNS 消息不超过512字节
- 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 |

| 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

# 针对根域名服务器的DDoS攻击


## 21 Oct 2002 Root Server Denial of Service Attack – Report

ISC/UMD/Cogent Paul Vixie, ISC OCTOBER21.TXT Gerry Sneeringer, UMD November 24, 2002 Mark Schleifer, Cogent

***Events of 21-Oct-2002***

**Abstract**: On October 21, 2002, the Internet Domain Name System's root name servers sustained a denial of service attack. This report explains the nature and impact of the attack, based on previously and publically available information.

### Nature of Attack

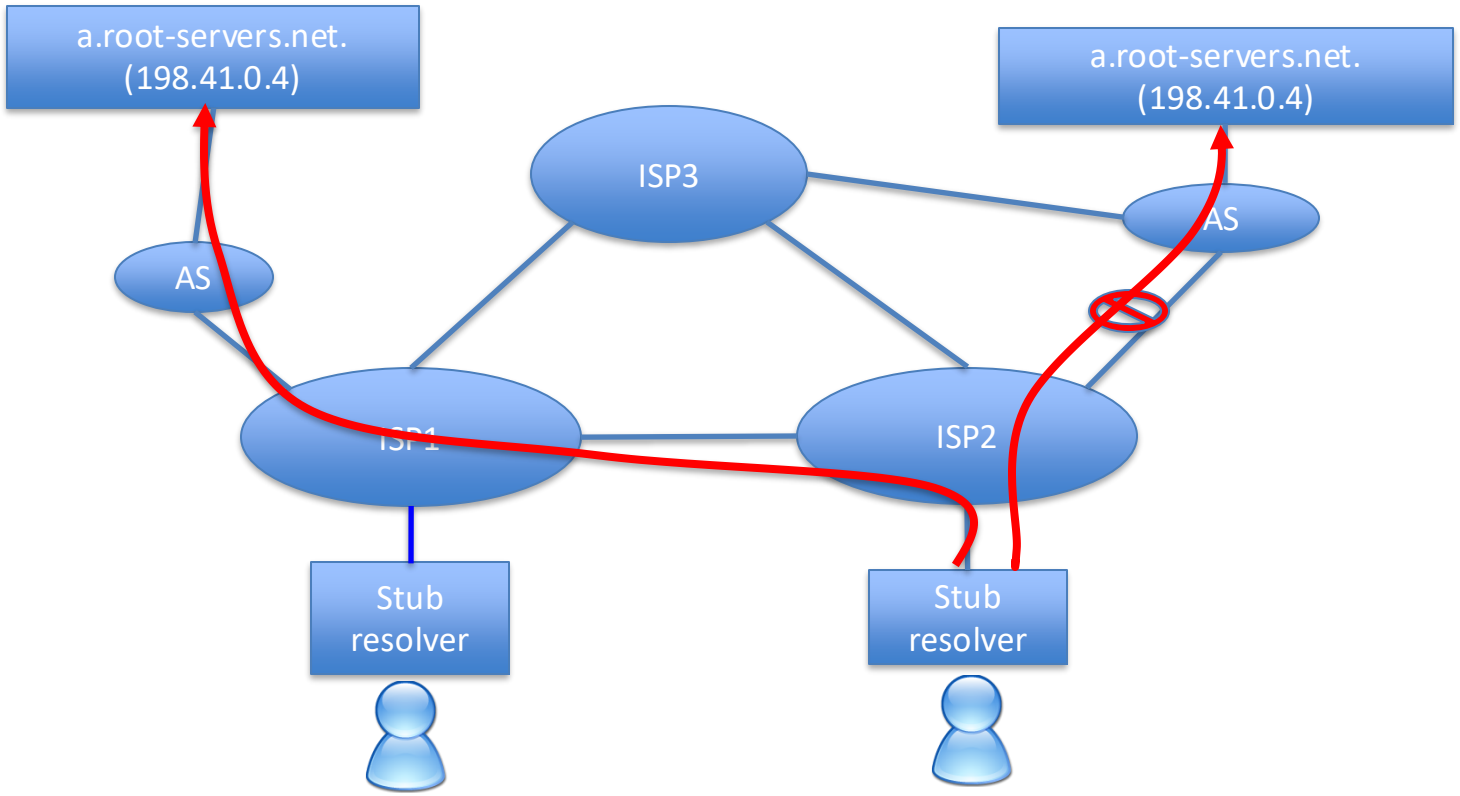
- A coordinated DDoS (distributed denial of service) attack was launched at approximately 2045UTC and lasted until approximately 2200UTC. All thirteen (13) DNS root name servers were targeted simultaneously.
- Attack volume was approximately 50 to 100 Mbits/sec (100 to 200 Kpkts/sec) per root name server, yielding a total attack volume was approximately 900 Mbits/sec (1.8 Mpkts/sec).
- Attack traffic contained ICMP, TCP SYN, fragmented TCP, and UDP.
- Attack source addresses were mostly randomized, chosen within netblocks which were mostly present in the routing table at the time of the attack.

### Impact of Attack

- Some root name servers were unreachable from many parts of the global Internet due to congestion from the attack traffic delivered upstream/nearby. While all servers continued to answer all queries they received (due to successful overprovisioning of host resources), many valid queries were unable to reach some root name servers due to attack-related congestion effects, and thus went unanswered.
- Several root name servers were reachable by inside-metro queries but not from outside-metro, due to attack-related congestion on wide area links connecting that metro to other parts of the world wide Internet.
- Several root name servers were continuously reachable from virtually all monitoring stations for the entire duration of the attack, due to successful overprovisioned at the network level (through a combination of multiple locations, fat pipes, hardware switched load balancing, and high path splay).
- There are no known reports of end-user visible error conditions during, and as a result of, this attack. Because the DNS protocol is designed to cope with partial reachability among a set of name servers, there may have been a minor delay (on the order of several seconds) for some name lookups. This would have manifested itself as a barely perceptible initial delay in some web browsers or other client programs (such as "ftp" or "ssh").
- Wide scale visibility of this attack came about only as a result of health monitoring projects around the Internet, usually in the form of "strip chart" graphics showing response time variance of a periodic, simple query against some set of servers, including root name servers.

### Analysis

# AnyCast Root Instance

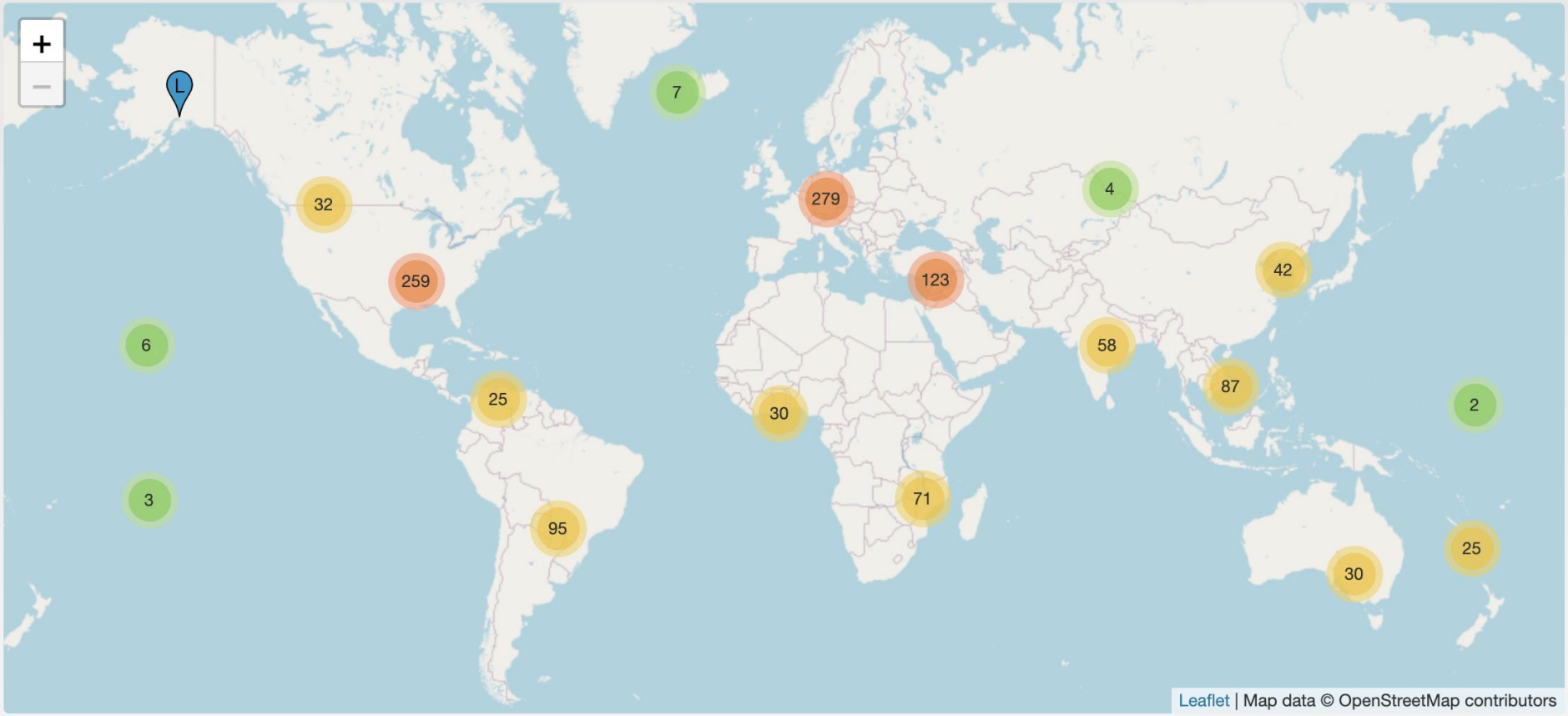





**RFC 3258, Distributing Authoritative Name Servers via Shared Unicast Addresses, 2002**

# Root Name Servers

- 根结点(Root Instance): 1404 by 10/07/2021




As of 10/07/2021 10:41 a.m., the root server system consists of 1404 instances operated by the 12 independent root server operators.

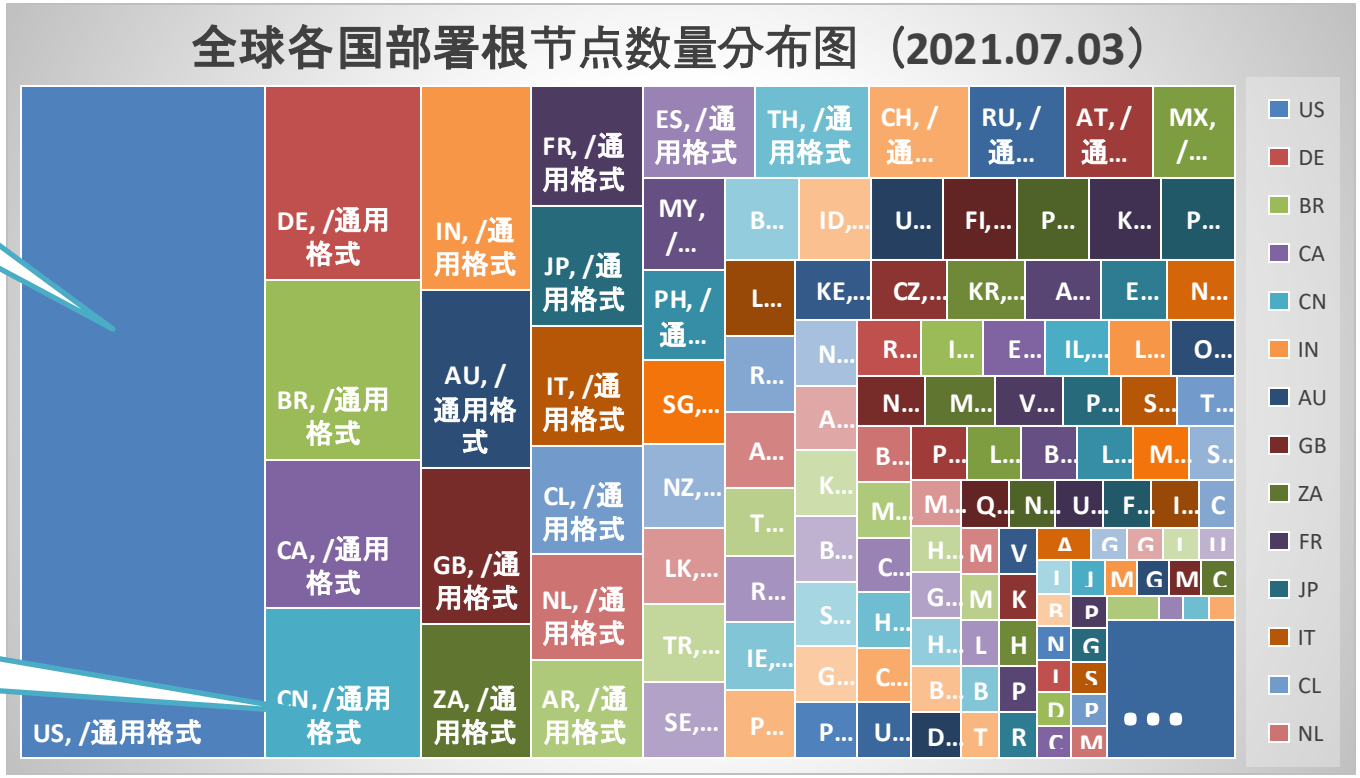
# DNS根节点在世界各国的分布

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

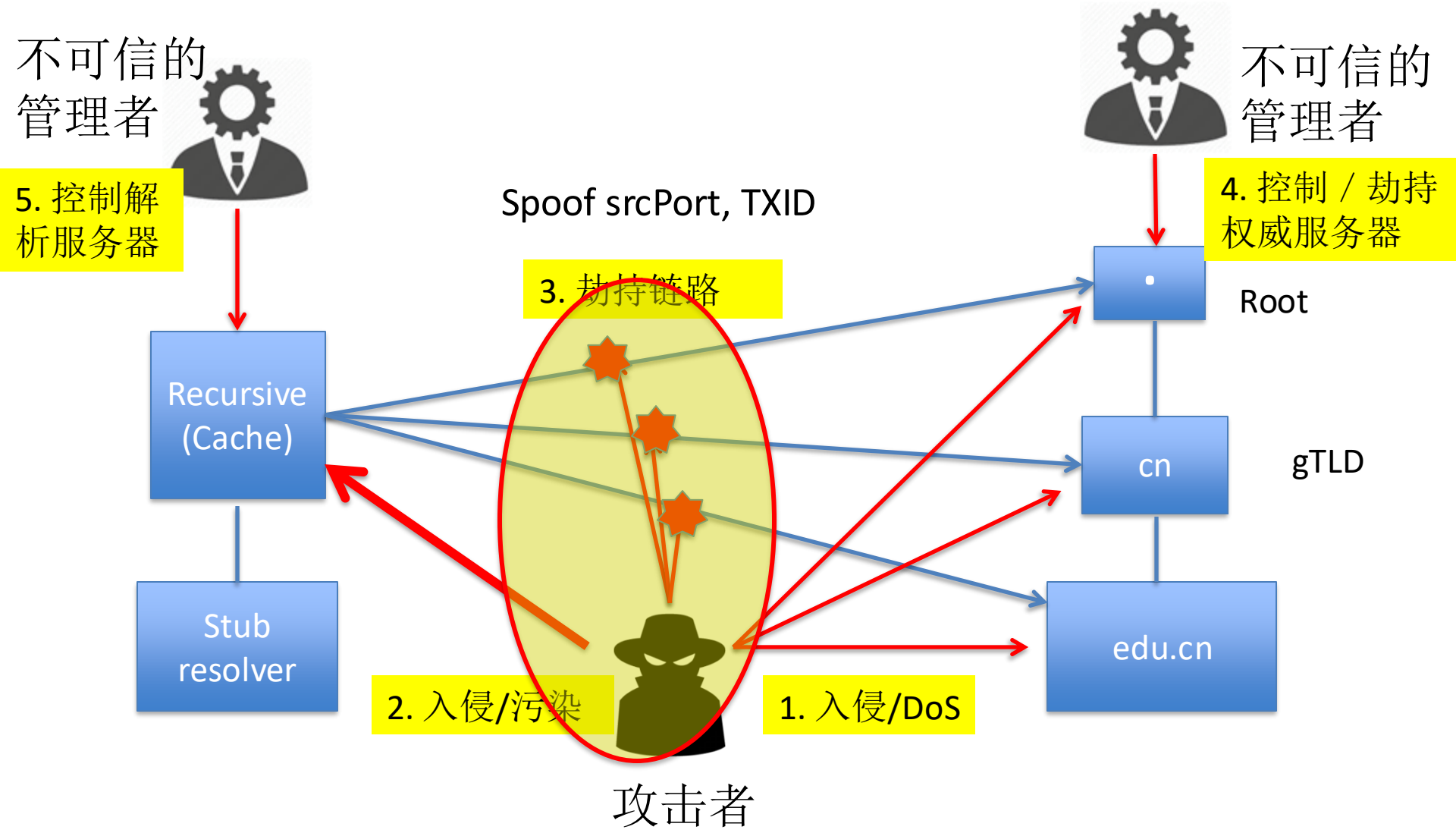
美国根节点281，
占全球20%

中国根节点40，
只占2.8%



# Who is answering my DNS query?

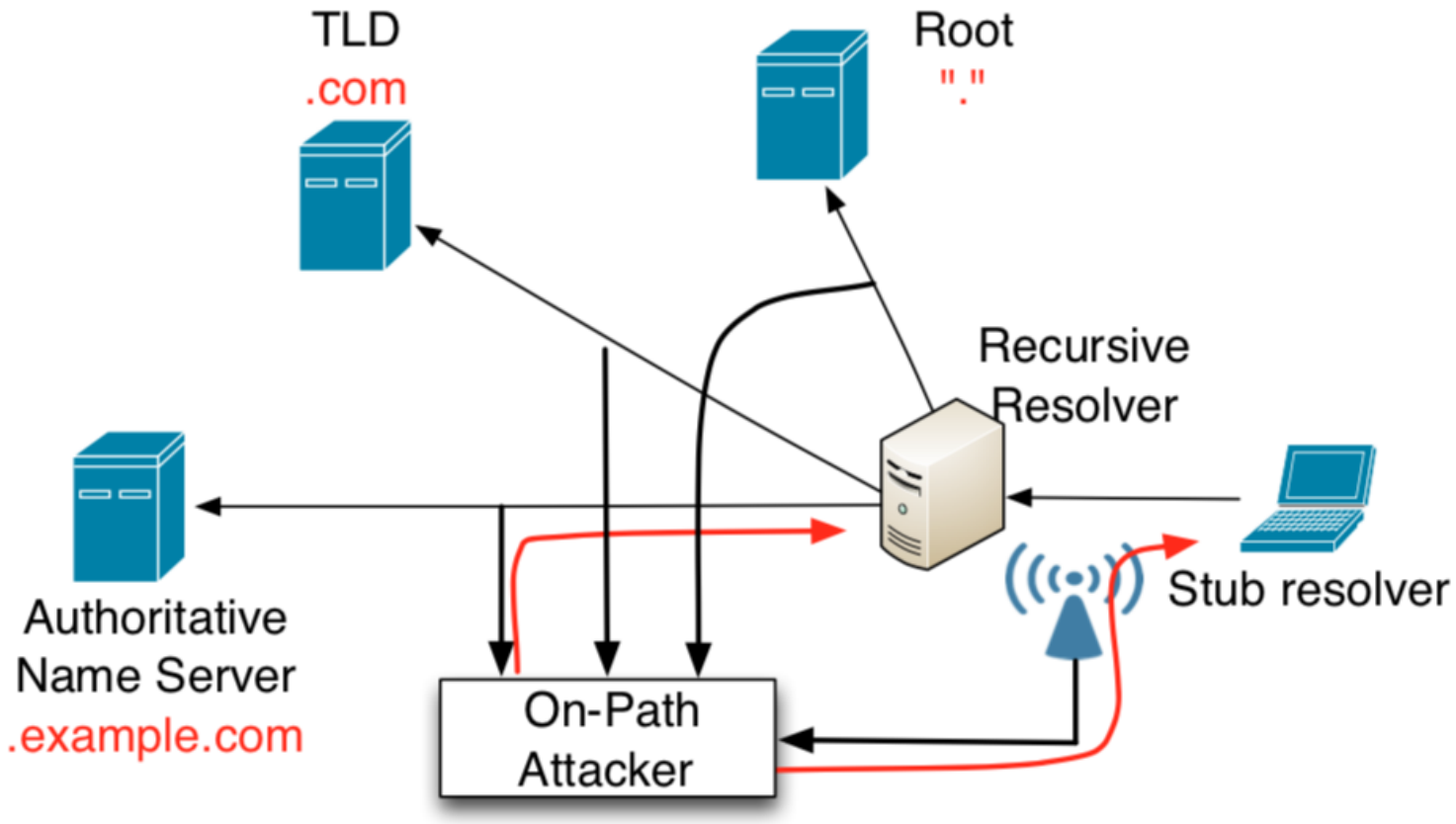
# DNS信任的攻击面（attack surface）



# On-Path Attackers



- Any path of the recursive resolution may be vulnerable



```
[duanhx@ccert ~]$ dig @8.8.8.8 www.youtube.com

; <<>> DiG 9.9.2 <<>> @8.8.8.8 www.youtube.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54941
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.youtube.com.               IN      A

;; ANSWER SECTION:
www.youtube.com.        2155    IN      A       8.7.198.45

;; Query time: 27 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct  7 18:44:49 2016
;; MSG SIZE  rcvd: 64
```

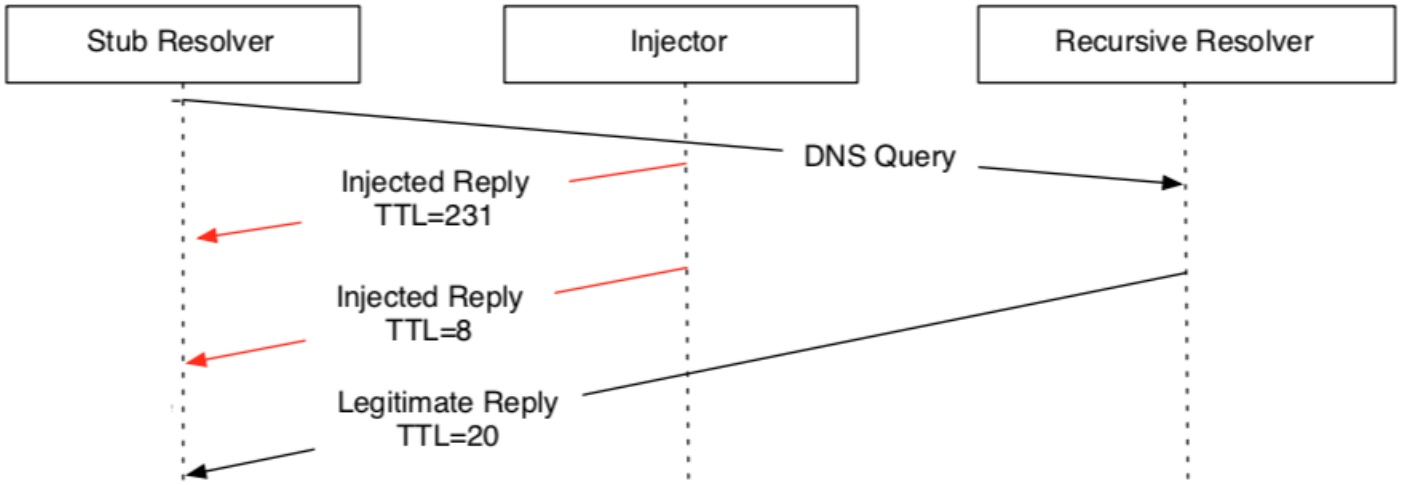
```
[duanhx@ccert ~]$ dig @8.8.8.8 www.mit.edu

; <<>> DiG 9.9.2 <<>> @8.8.8.8 www.mit.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18694
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.mit.edu.                   IN      A

;; ANSWER SECTION:
www.mit.edu.            1799    IN      CNAME   www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net. 59     IN      CNAME   e9566.dscb.akamaiedge.net.
e9566.dscb.akamaiedge.net. 19   IN      A       23.220.189.48

;; Query time: 164 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct  7 18:47:17 2016
;; MSG SIZE  rcvd: 129
```

```
[duanhx@ccert ~]$ dig @www.mit.edu twitter.com

; <<>> DiG 9.11.0-P1 <<>> @www.mit.edu twitter.com
; (3 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45230
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;twitter.com.                   IN      A

;; ANSWER SECTION:
twitter.com.            94      IN      A       8.7.198.45

;; Query time: 101 msec
;; SERVER: 23.77.14.148#53(23.77.14.148)
;; WHEN: Wed Oct 11 20:29:52 CST 2017
;; MSG SIZE  rcvd: 45

[duanhx@ccert ~]$ dig @www.mit.edu www.youtube.com

; <<>> DiG 9.11.0-P1 <<>> @www.mit.edu www.youtube.com
; (3 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21264
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.youtube.com.               IN      A

;; ANSWER SECTION:
www.youtube.com.        206     IN      A       59.24.3.173

;; Query time: 102 msec
;; SERVER: 23.77.14.148#53(23.77.14.148)
;; WHEN: Wed Oct 11 20:30:06 CST 2017
;; MSG SIZE  rcvd: 49
```

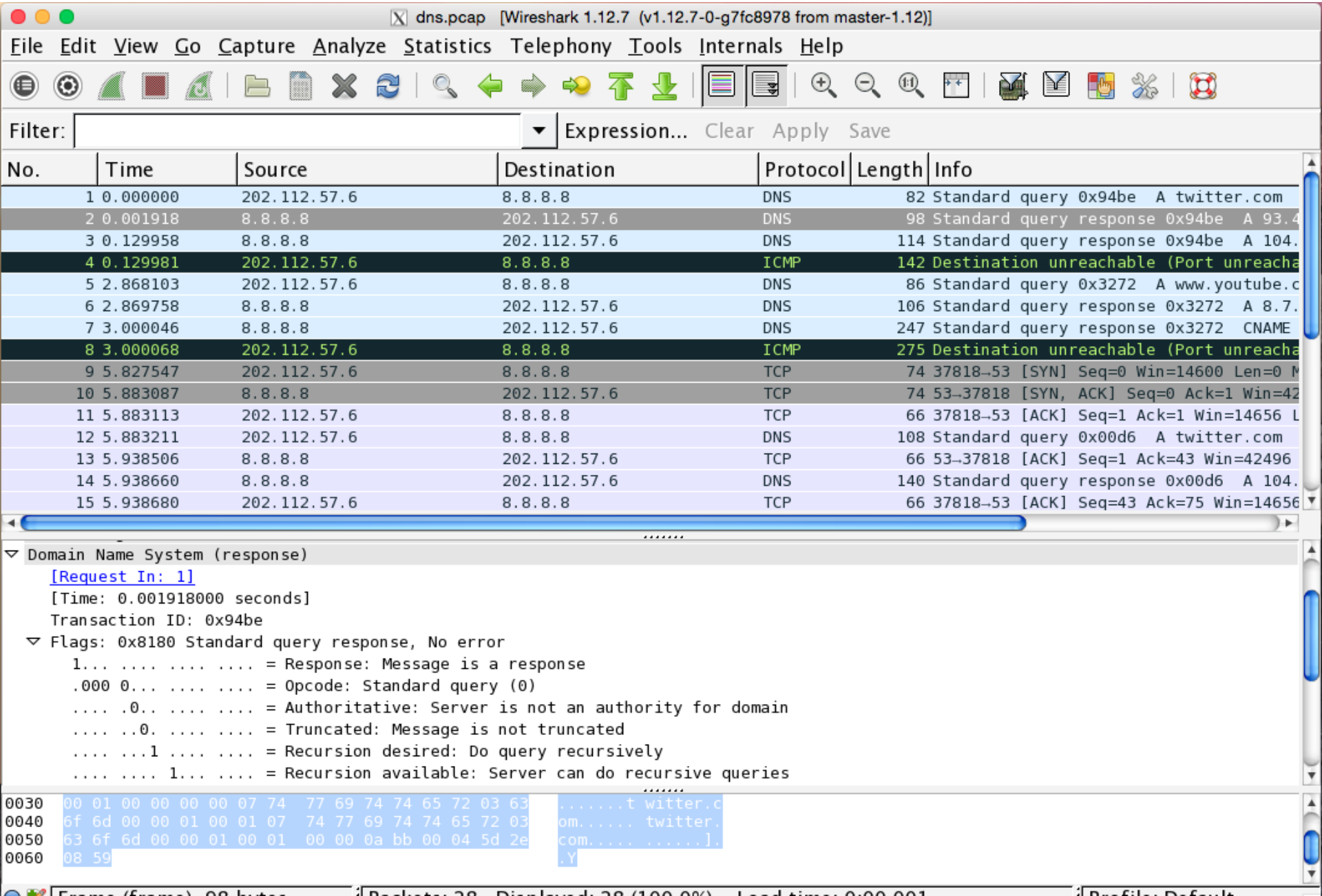
# A Key Property



- On-path attackers can't suppress the legitimate reply
  - Otherwise, they would be an in-path attacker




```
root@ubuntu:~# tcpdump -r dns.pcap -n
reading from file dns.pcap, link-type EN10MB (Ethernet)
10:14:30.765462 IP 202.112.51.35.44847 > 8.8.8.8.53: 11805+ [1au] A? twitter.com. (52)
10:14:30.766253 IP 8.8.8.8.53 > 202.112.51.35.44847: 11805 1/0/0 A 69.171.245.84 (45)
10:14:30.766366 IP 8.8.8.8.53 > 202.112.51.35.44847: 11805 1/0/0 A 69.171.234.29 (45)
10:14:31.008695 IP 8.8.8.8.53 > 202.112.51.35.44847: 11805 2/0/1 A 104.244.42.129, A 104.244.42.1 (72)
10:14:31.008730 IP 202.112.51.35 > 8.8.8.8: ICMP 202.112.51.35 udp port 44847 unreachable, length 108
```


dns.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 202.112.57.6 8.8.8.8 DNS 82 Standard query 0x94be A twitter.com
2 0.001918 8.8.8.8 202.112.57.6 DNS 98 Standard query response 0x94be A 93.4
3 0.129958 8.8.8.8 202.112.57.6 DNS 114 Standard query response 0x94be A 104.
4 0.129981 202.112.57.6 8.8.8.8 ICMP 142 Destination unreachable (Port unreacha
5 2.868103 202.112.57.6 8.8.8.8 DNS 86 Standard query 0x3272 A www.youtube.c
6 2.869758 8.8.8.8 202.112.57.6 DNS 106 Standard query response 0x3272 A 8.7.
7 3.000046 8.8.8.8 202.112.57.6 DNS 247 Standard query response 0x3272 CNAME
8 3.000068 202.112.57.6 8.8.8.8 ICMP 275 Destination unreachable (Port unreacha
9 5.827547 202.112.57.6 8.8.8.8 TCP 74 37818→53 [SYN] Seq=0 Win=14600 Len=0 M
10 5.883087 8.8.8.8 202.112.57.6 TCP 74 53→37818 [SYN, ACK] Seq=0 Ack=1 Win=42
11 5.883113 202.112.57.6 8.8.8.8 TCP 66 37818→53 [ACK] Seq=1 Ack=1 Win=14656 L
12 5.883211 202.112.57.6 8.8.8.8 DNS 108 Standard query 0x00d6 A twitter.com
13 5.938506 8.8.8.8 202.112.57.6 TCP 66 53→37818 [ACK] Seq=1 Ack=43 Win=42496
14 5.938660 8.8.8.8 202.112.57.6 DNS 140 Standard query response 0x00d6 A 104.
15 5.938680 202.112.57.6 8.8.8.8 TCP 66 37818→53 [ACK] Seq=43 Ack=75 Win=14656
Domain Name System (response)
[Request In: 1]
[Time: 0.001918000 seconds]
Transaction ID: 0x94be
Flags: 0x8180 Standard query response, No error
1... .... .... .... = Response: Message is a response
.000 0... .... .... = Opcode: Standard query (0)
.... .0.. .... .... = Authoritative: Server is not an authority for domain
.... ..0. .... .... = Truncated: Message is not truncated
.... ...1 .... .... = Recursion desired: Do query recursively
.... .... 1... .... = Recursion available: Server can do recursive queries
0030 00 01 00 00 00 00 07 74 77 69 74 74 65 72 03 63 .......t witter.c
0040 6f 6d 00 00 01 00 01 07 74 77 69 74 74 65 72 03 om...... twitter.
0050 63 6f 6d 00 00 01 00 01 00 00 0a bb 00 04 5d 2e com..... ......].
0060 08 59 .Y

# DNS Operation Mailing list,3/24/2010

Hi there! A local ISP has told us that there's some strange behavior with at least one node in i.root-servers.net (traceroute shows mostly China) It seems that when you ask A records for facebook, youtube or twitter, you get an IP and not the referral for .com

It doesn't happen every time, but we have confirmed this on 4 different connectivity places (3 in Chile, one in California)

This problem has been reported to Autonomica/Netnod but I don't know if anyone else is seeing this issue.

This is an example of what are we seeing:

$ dig @i.root-servers.net www.facebook.com A ;
….
ANSWER SECTION: www.facebook.com. 86400 IN A 8.7.198.45

Mauricio Vergara Ereche
Santiago CHILE

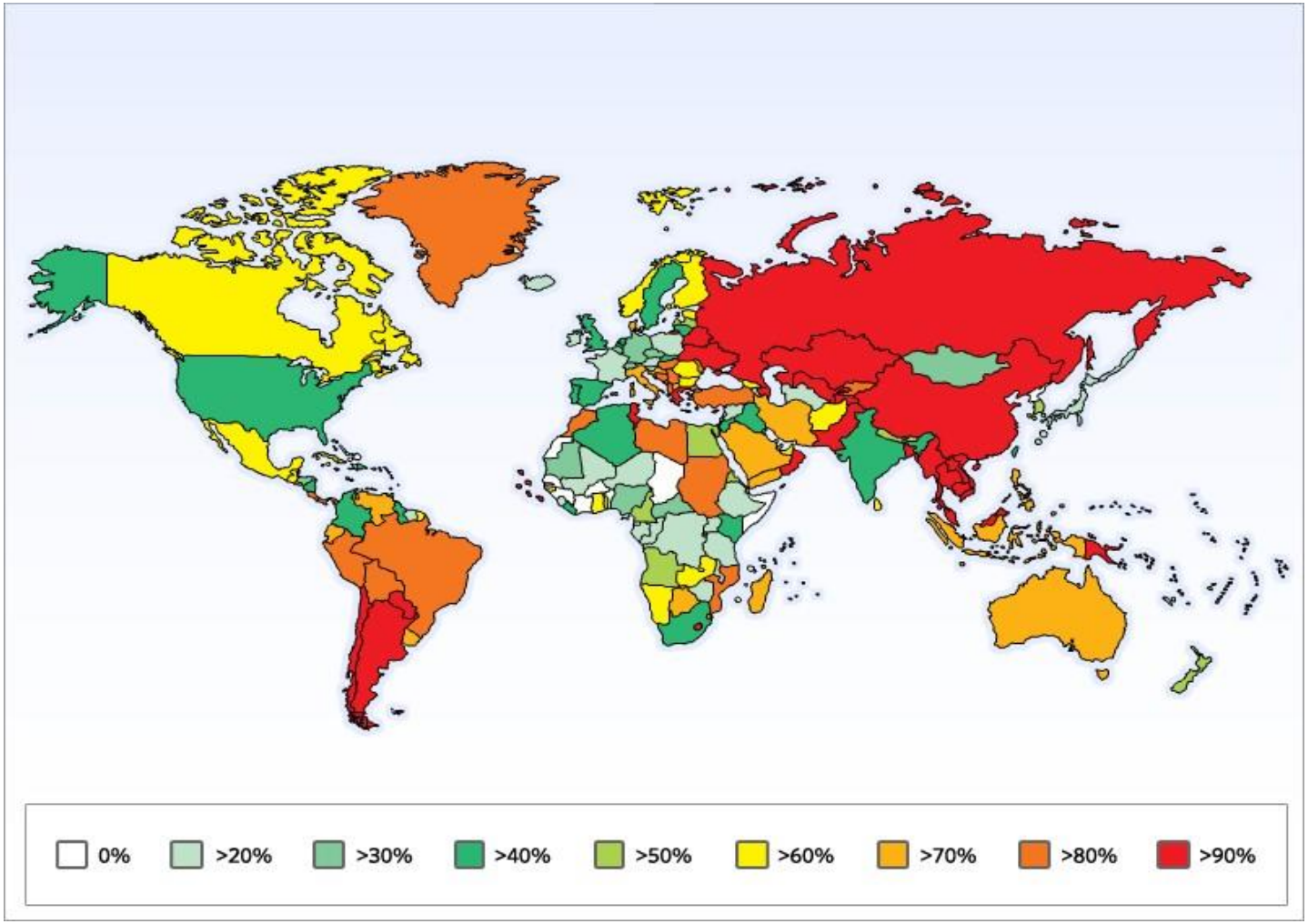
# Root Servers in CN Serve Global Internet

# Explanation

- The global advertisements for 192.36.148.0/24 include AS 29216 (I-root) and AS 8674 and then traversed several Chinese ASNs (in red).
- Inbound packets on this path would traverse AS 10026 (PacNet), AS 7497 (Computer Network Information Center), AS 24151 (CNNIC) before reaching AS 29216 and 8674:
  - […] 10026 7497 7497 24151 8674 29216
- Peers selecting this path would clearly be sending their queries to the Beijing node.
- The results reported by Mauricio Vergara Ereche on the dns-operations mailing list are consistent with GFW behavior.

http://www.renesys.com/tech/presentations/pdf/DNS-Tampering-and-Root-Servers.pdf

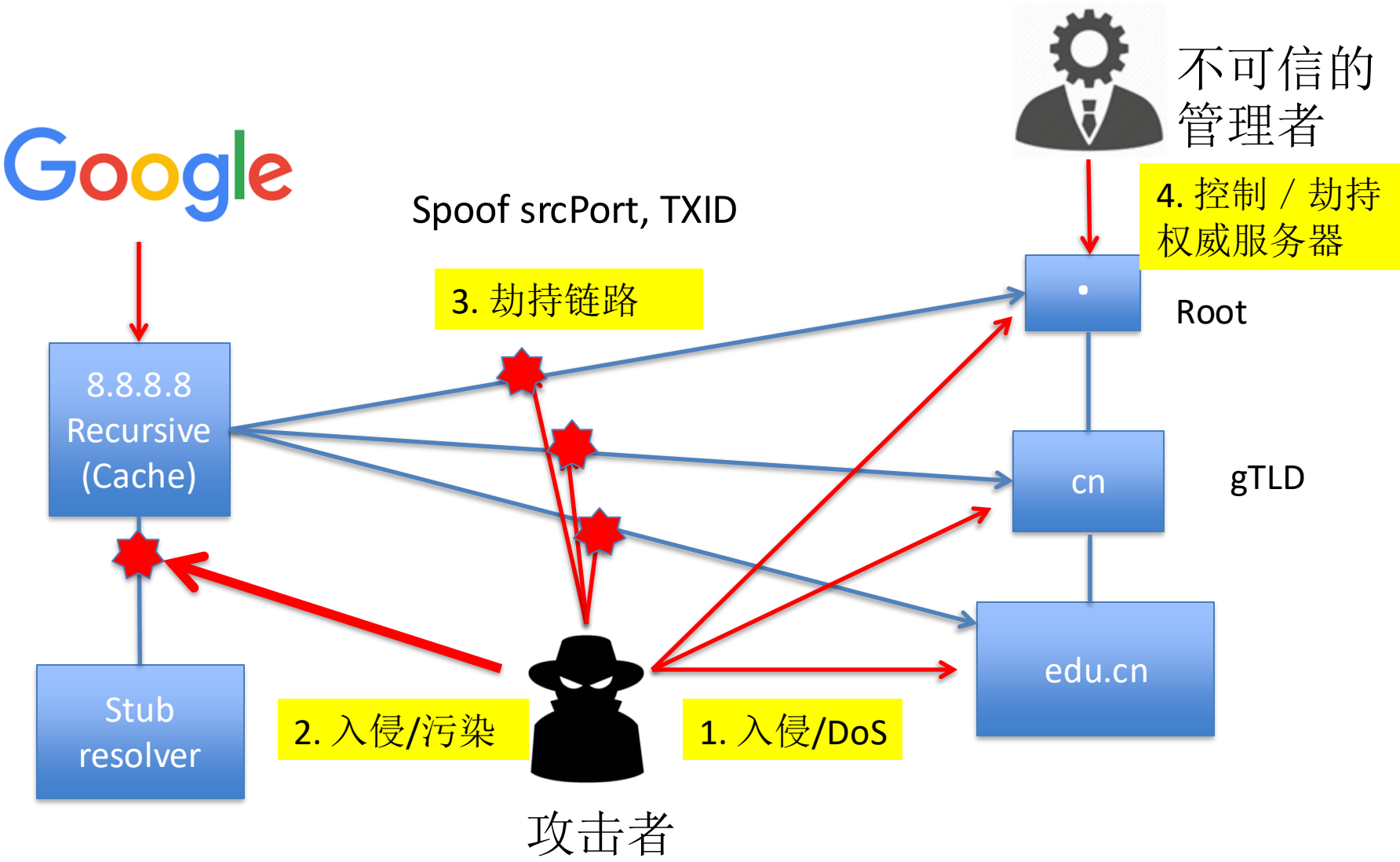
# Who could have been affected?



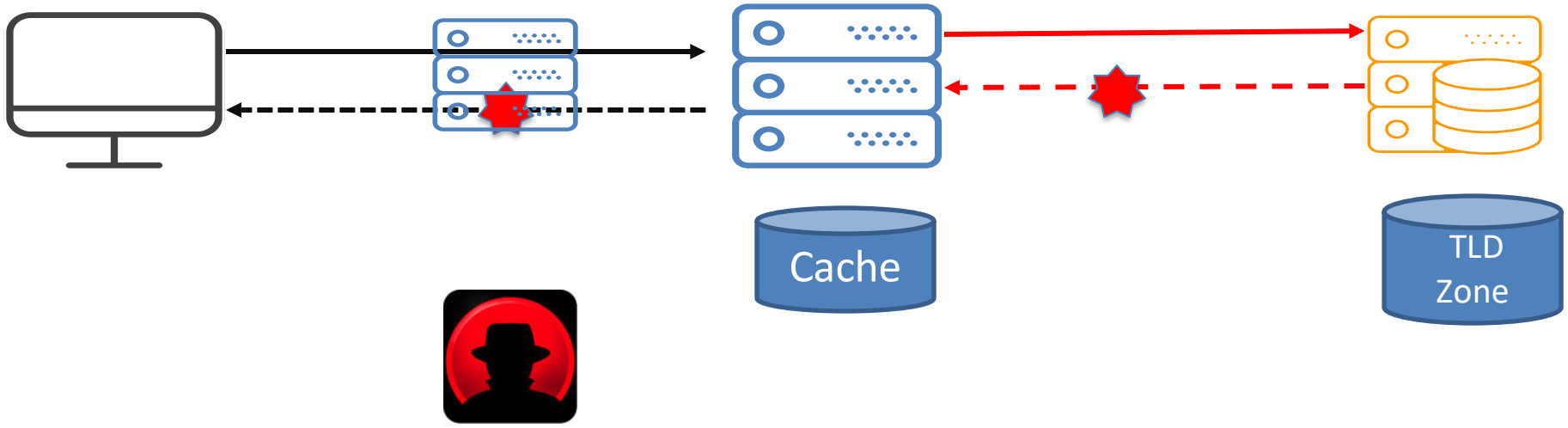
# Netnod serves Chinese market

- Netnod intends the Beijing node to be globally visible.
- Netnod employs TSIG and routinely checks serial numbers of the data at each of their root server instances against Verisign/IANA root zone data to ensure validity.
- The tampering of replies from the Beijing I-root was completely consistent with and almost irrefutably the GFW.
- Netnod withdrew their anycasted routes until their host (CNNIC) could secure assurances that the tampering would not recur.
- Netnod serves a large Internet user base in China and its Beijing node is one of its top 5 busiest instances.

# DNS信任的攻击面（attack surface）



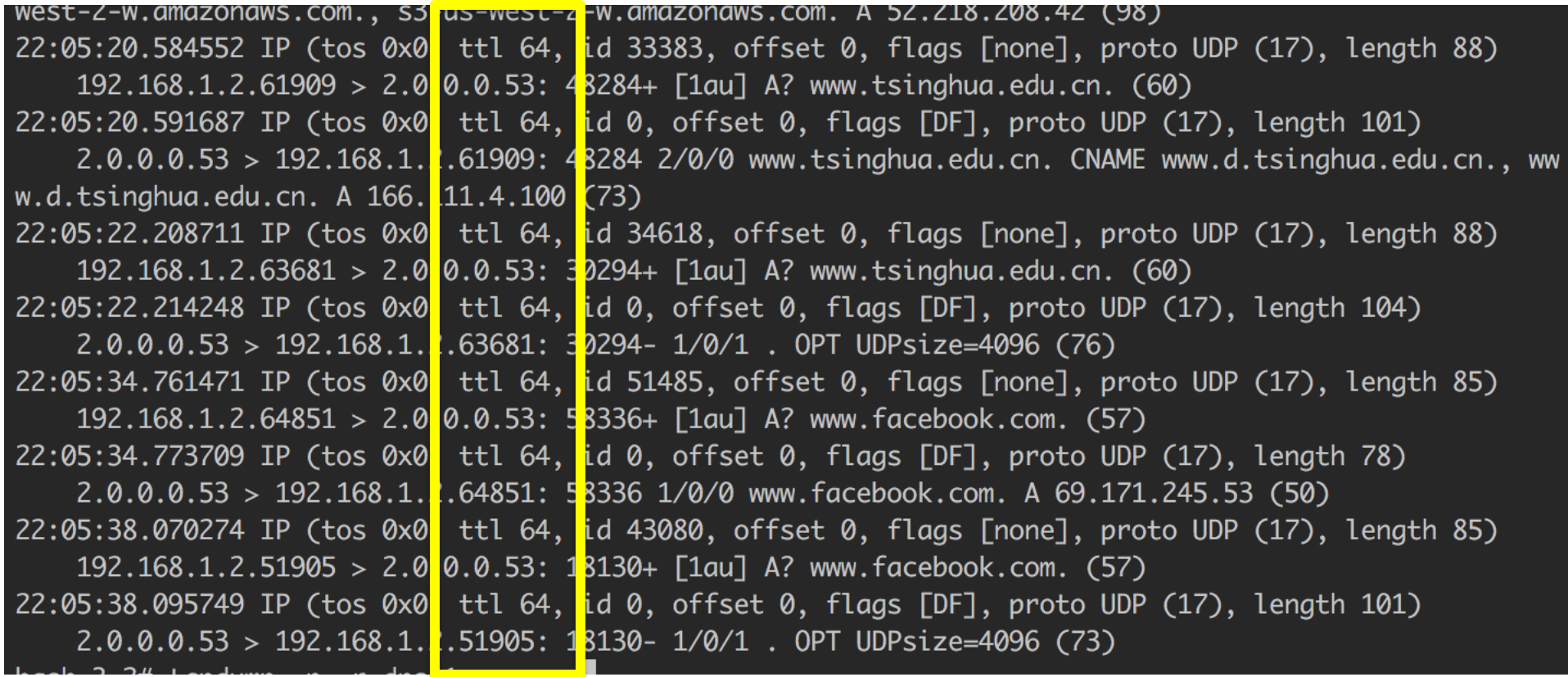
# DNS查询路径上的劫持/注入



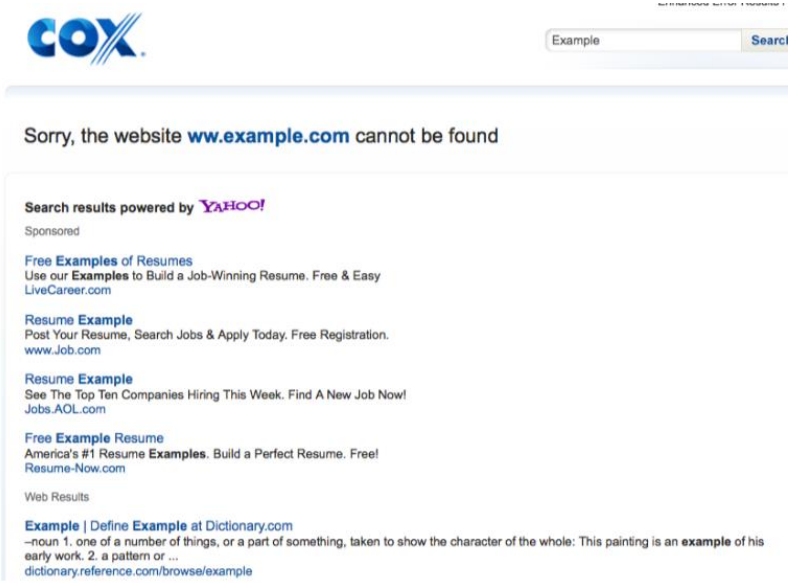

In Path 攻击者

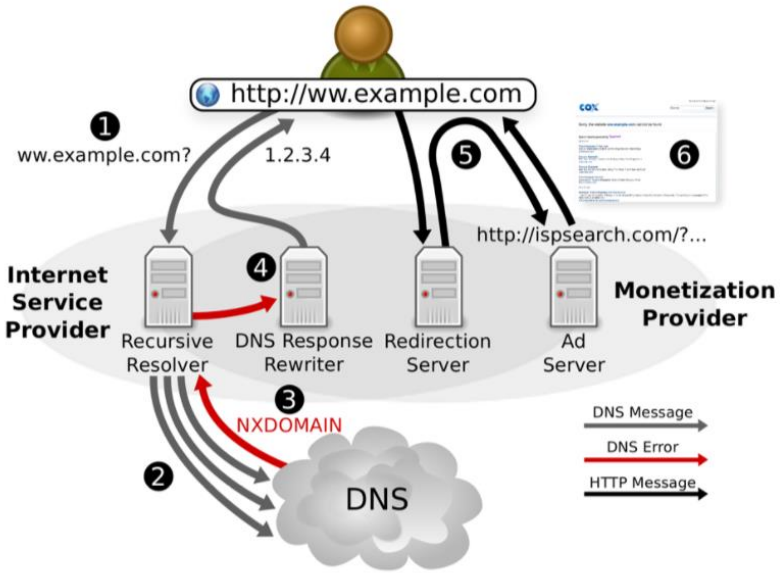
# 北京联通的家庭宽带

- 网关:192.168.1.1，我的地址： 192.168.1.2
- $ dig @2.0.0.0  www.tsinghua.edu.cn



# DNS Error Monetization employed by ISP




ISPs will see profits of 1–3 USD per customer per year

ICANN has criticized this practice due to its potential to cause both security and stability problems

N. Weaver, V. Paxson, and C. Kreibich, “Redirecting DNS for Ads and Profit,” FOCI 2011.

# 使用公共DNS服务，据说他们更安全

Google Public DNS　OpenDNS　CLOUDFLARE 1.1.1.1 DNS　114DNS

Why should you try Google Public DNS?

Speed up your browsing experience

Improve your security

DNSSEC

DNS over HTTPS

Get the results you expect with absolutely no redirection

Privacy First: Guaranteed.

We will never sell your data or use it to target ads. Period.

DNS over TLS， DNS over HTTPS

# FB宕机事件，许多用户把DNS切换到Google

## Facebook: More details about the October 4 outage

This was the source of yesterday's outage. During one of these routine maintenance jobs, a command was issued with the intention to assess the availability of global backbone capacity, which unintentionally took down all the connections in our backbone network, effectively disconnecting Facebook data centers globally. Our systems are designed to audit commands like these to prevent mistakes like this, but a bug in that audit tool prevented it from properly stopping the command.

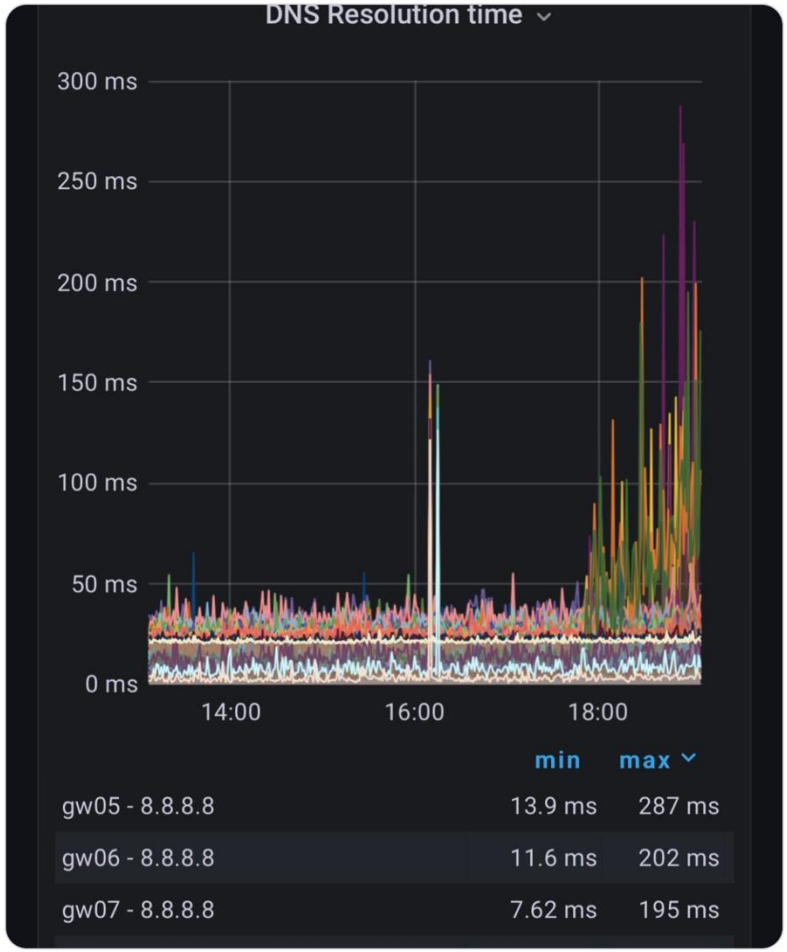
This change caused a complete disconnection of our server connections between our data centers and the internet. And that total loss of connection caused a second issue that made things worse.

One of the jobs performed by our smaller facilities is to respond to DNS queries. DNS is the address book of the internet, enabling the simple web names we type into browsers to be translated into specific server IP addresses. Those translation queries are answered by our authoritative name servers that occupy well known IP addresses themselves, which in turn are advertised to the rest of the internet via another protocol called the border gateway protocol (BGP).

To ensure reliable operation, our DNS servers disable those BGP advertisements if they themselves can not speak to our data centers, since this is an indication of an unhealthy network connection. In the recent outage the entire backbone was removed from operation, making these locations declare themselves unhealthy and withdraw those BGP advertisements. The end result was that our DNS servers became unreachable even though they were still operational. This made it impossible for the rest of the internet to find our servers.

#GoogleDNS 8.8.8.8 becomes much slower because of #Facebookdown and all the client retries.

翻译推文



Does your DNS response really come from the server you assigned ?

27th USENIX Security Symposium Aug. 15-17, 2018, Baltimore, MD, USA

# **Who Is Answering My Queries:** Understanding and Characterizing Interception of the DNS Resolution Path

Baojun Liu, Chaoyi Lu, Haixin Duan, Ying Liu, Zhou Li, Shuang Hao, Min Yang

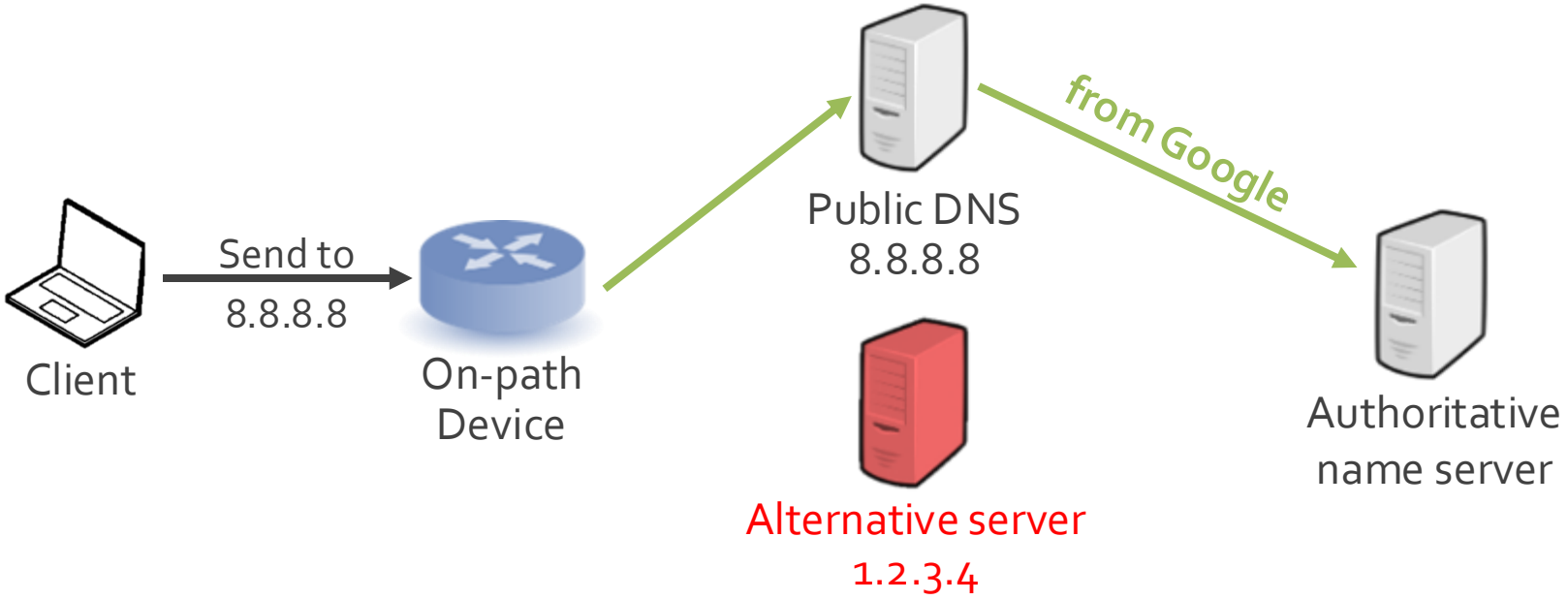
清華大學 Tsinghua University

UT DALLAS Fitness

復旦大學 FUDAN UNIVERSITY

# Normal DNS resolution

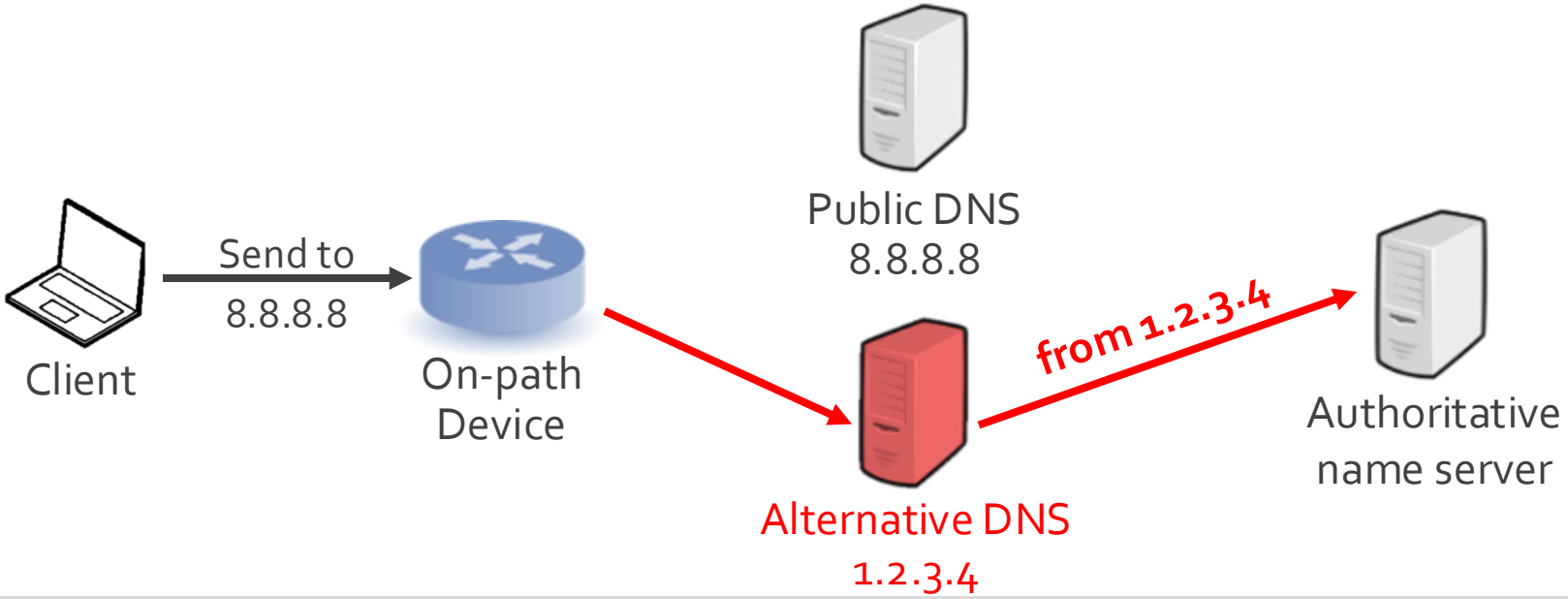
- We setup our own authoritative name server
- Normally, we can see one query from Google




Baojun L., Chaoyi L., HaiXin D., Ying L., Zhou L., Shuang H., Min Y: Who Is Answering My Queries. USENIX Sec 2018

# DNS interception 1: Redirection

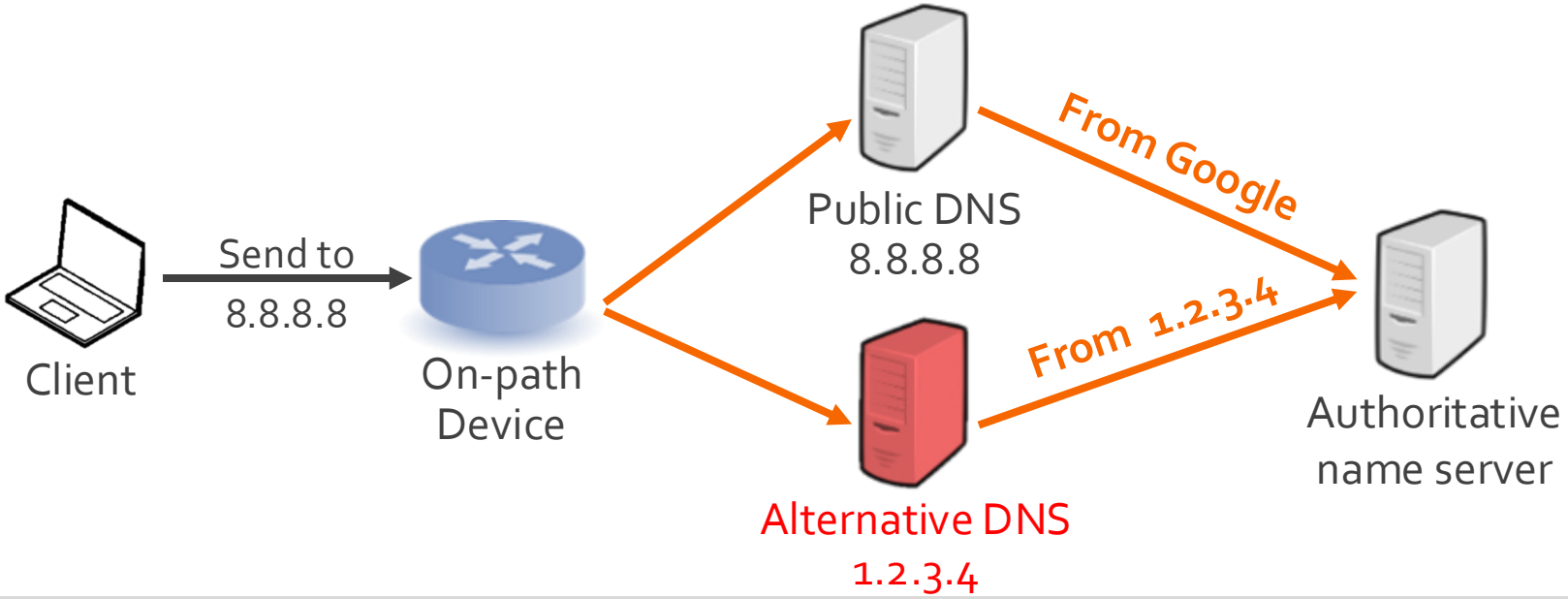
- Authoritative server receive one query, but from a different address, outside of Google




Baojun L., Chaoyi L., HaiXin D., Ying L., Zhou L., Shuang H., Min Y: Who Is Answering My Queries. USENIX Sec 2018

# DNS interception 2： replication

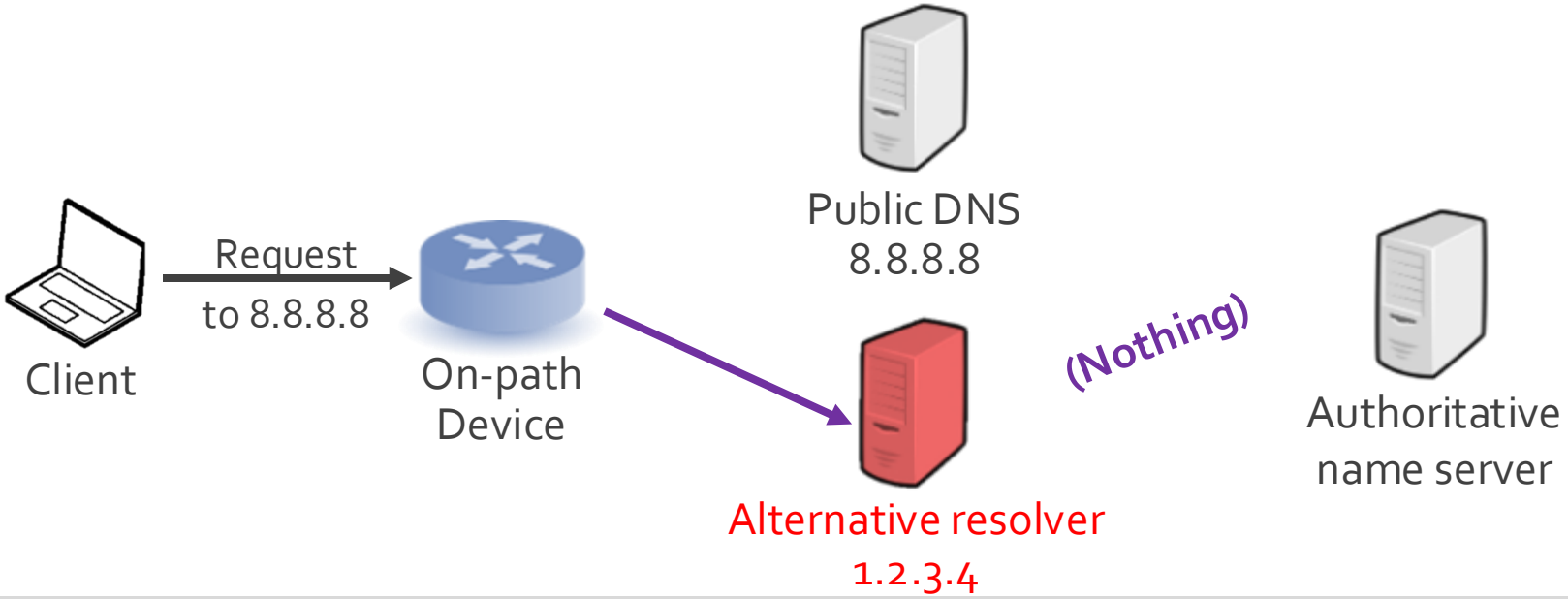
- Authoritative server receives two queries, one from Google, the other from unknow third party.




Baojun L., Chaoyi L., HaiXin D., Ying L., Zhou L., Shuang H., Min Y: Who Is Answering My Queries. USENIX Sec 2018

# DNS interception 3: reply directly

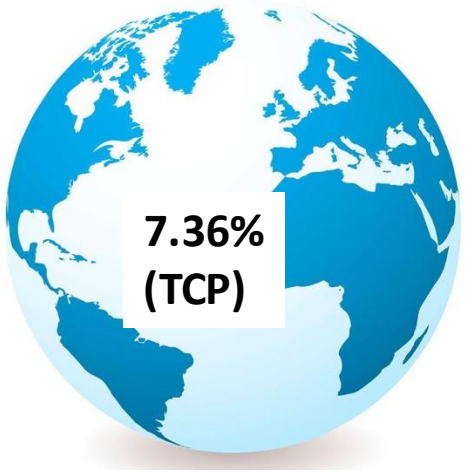
- Authoritative name server get nothing, but the client get an answer (every queried name is unique, no caching)

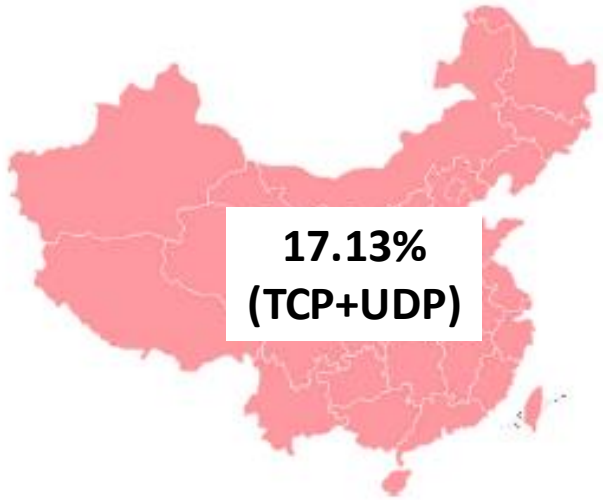



Baojun L., Chaoyi L., HaiXin D., Ying L., Zhou L., Shuang H., Min Y: Who Is Answering My Queries. USENIX Sec 2018

# Articles about controlling DNS queries to other ISPs


# Global measurement of interception of DNS resolution



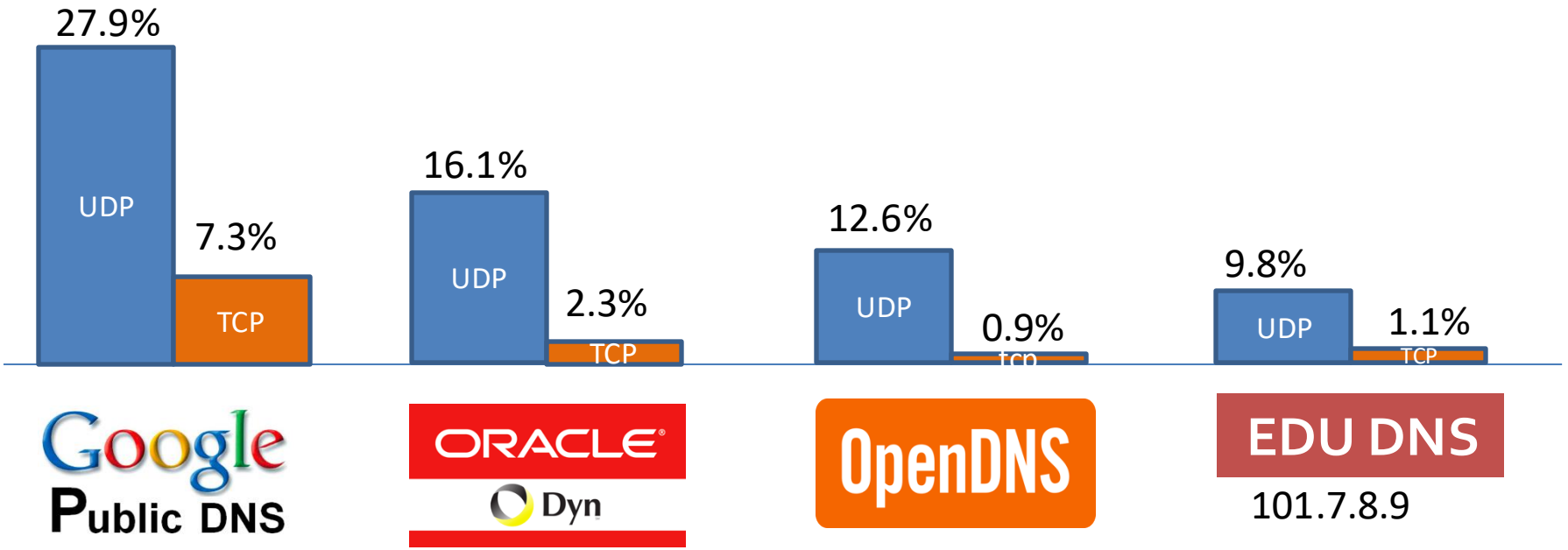

Global measurement:
Interception detected in 198/2,691 ASes

China Measurement:
Interception detected in 61/356 ASes

Baojun L., Chaoyi L., HaiXin D., Ying L., Zhou L., Shuang H., Min Y: Who Is Answering My Queries. USENIX Sec 2018

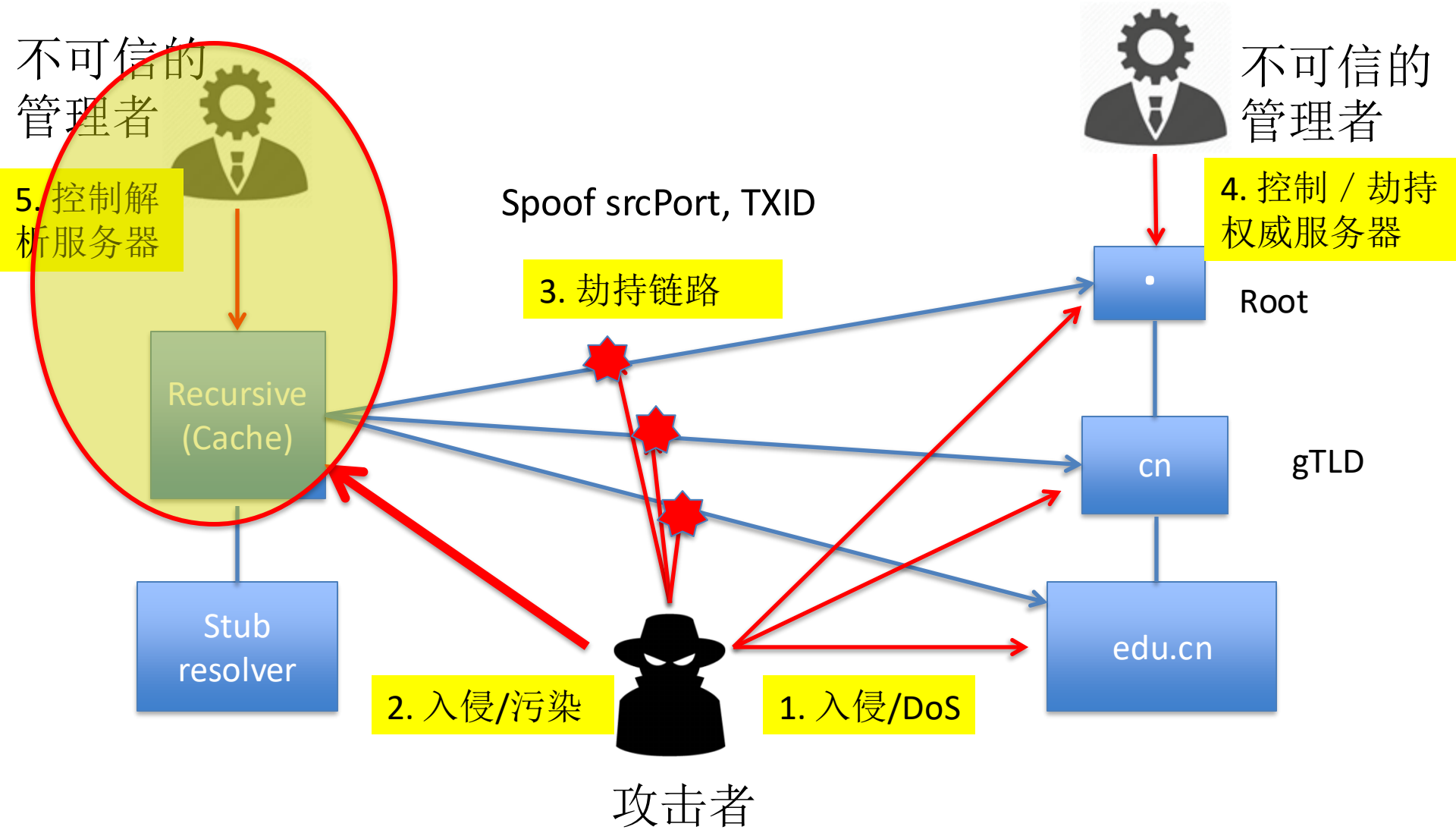
# Popular Public DNS Services Intercepted

- More popular, more interception
- DNS over TCP is unlikely to be intercepted

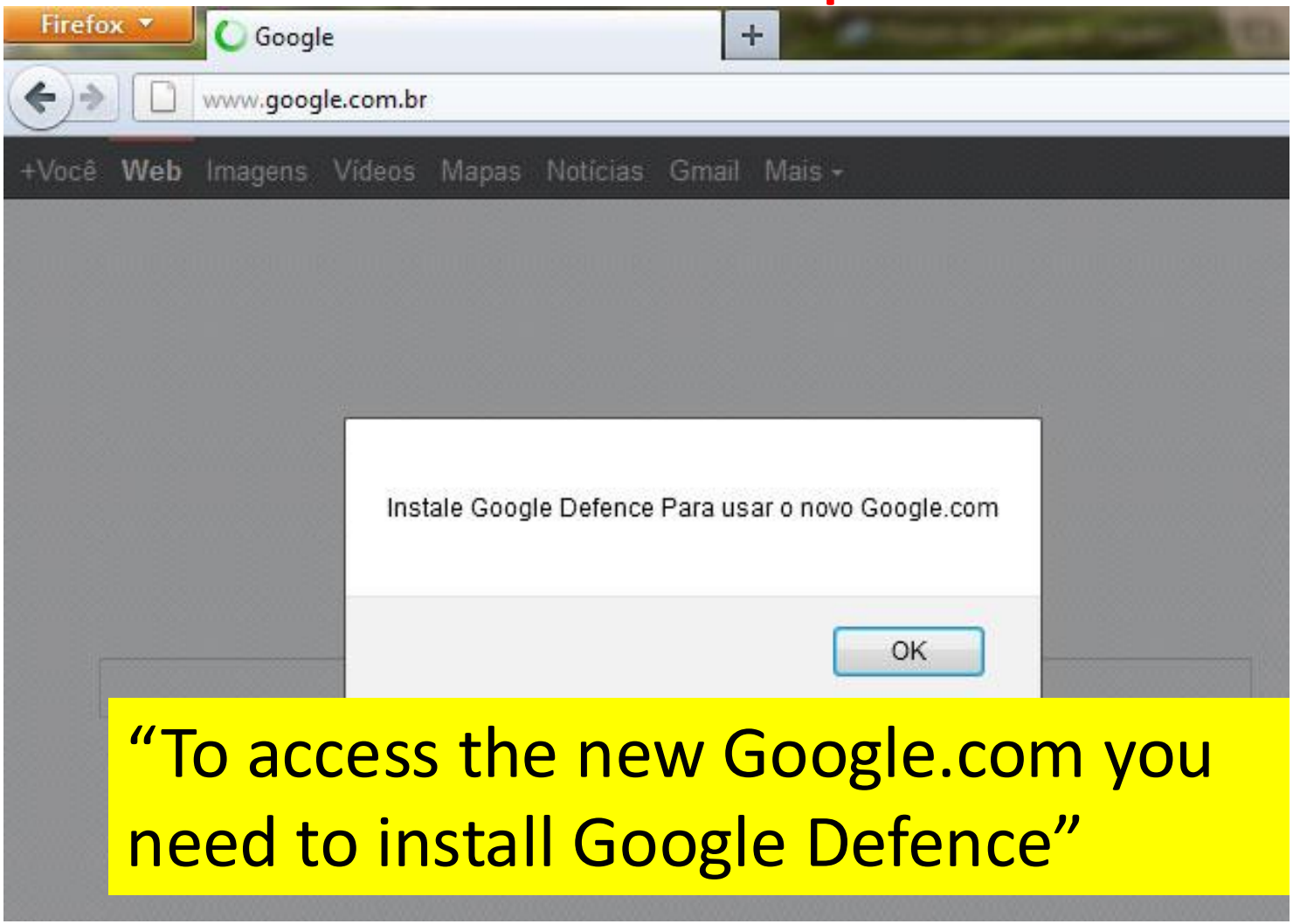



Baojun L., Chaoyi L., HaiXin D., Ying L., Zhou L., Shuang H., Min Y: Who Is Answering My Queries. USENIX Sec 2018

# DNS信任的攻击面（attack surface）

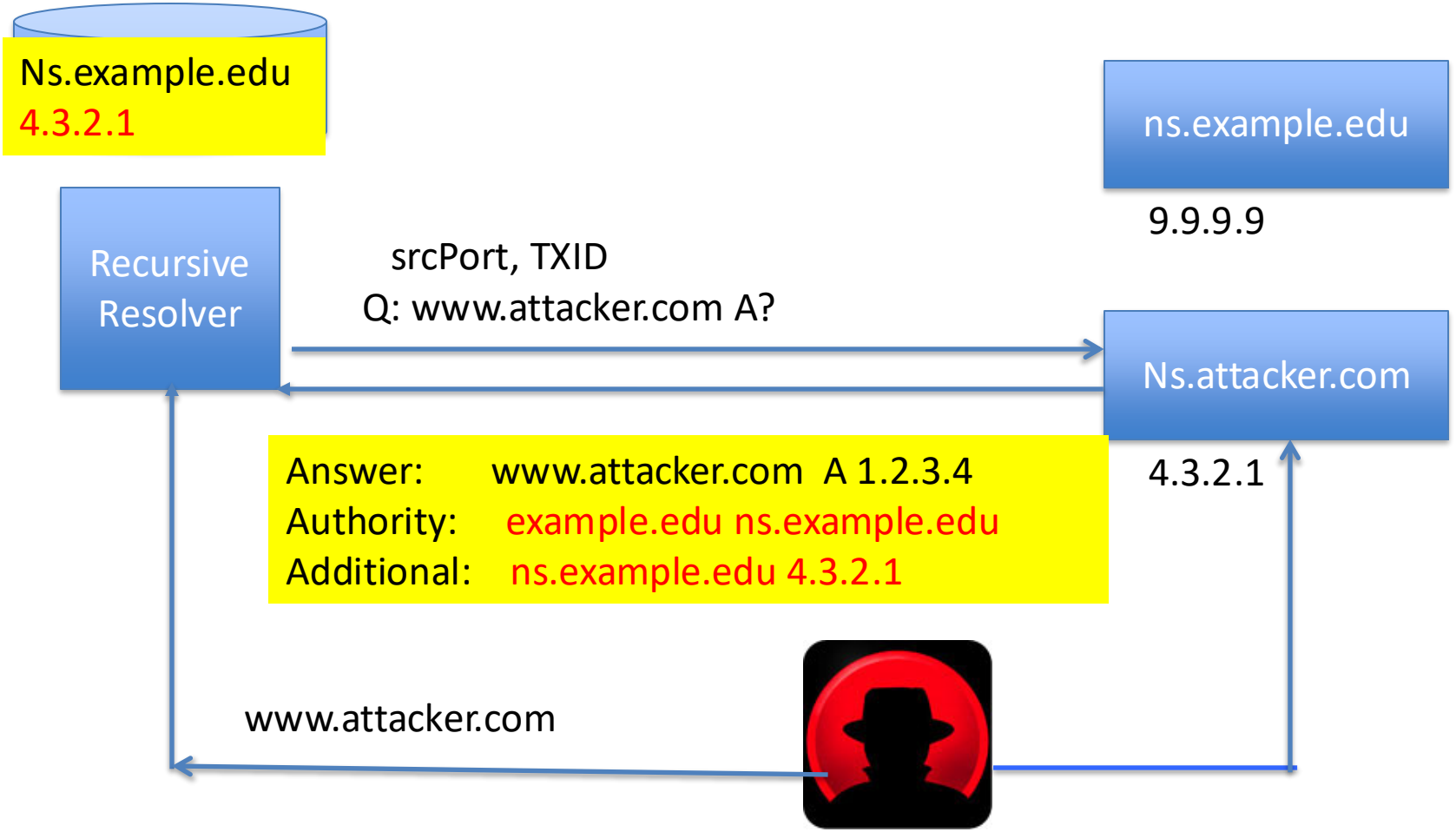


# Brazillian ISP's DNS cache poisoned 2011




http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil

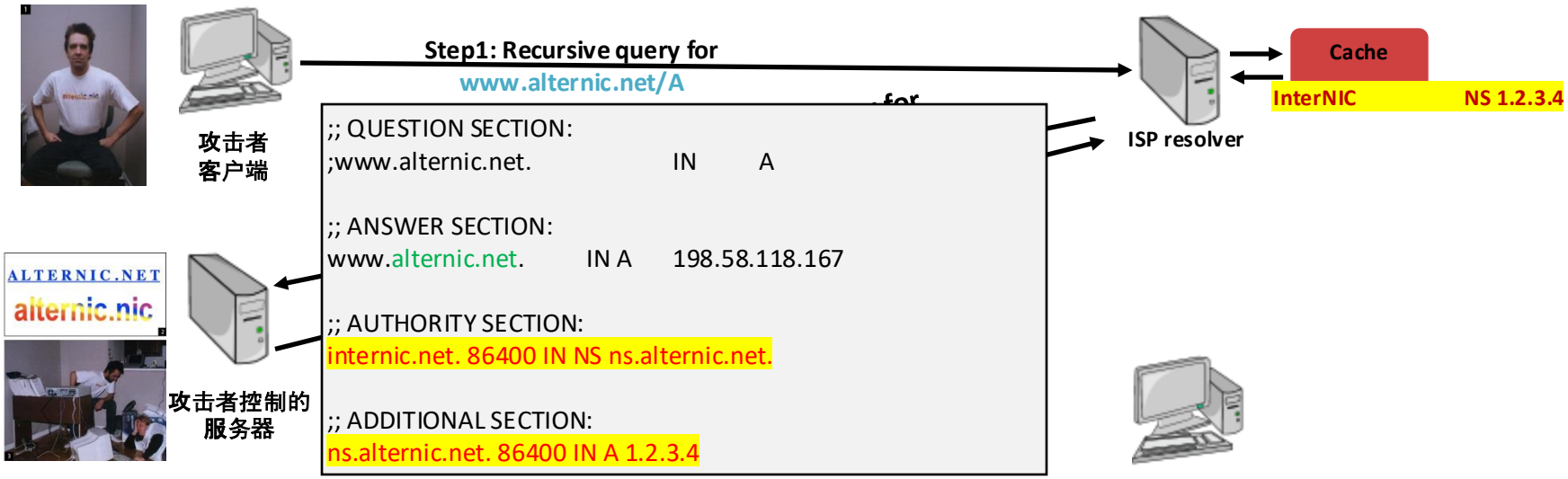
# Cache Poisoning: Old attack




1999, Daniel J. Bernstein, **Notes on the Domain Name System,** http://cr.yp.to/djbdns/notes.html

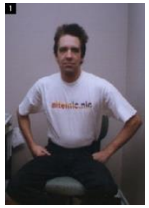
# 攻击1：Kashpureff 攻击，1997

- **历史背景： 90年代域名的战争——InterNIC 与 AlterNIC的冲突**
  - **攻击方案**：直接从**权威服务器处**回复虚假响应，解析器相信并**缓存所有回复**的资源记录
  - **漏洞成因**：**缺乏数据验证**



# 攻击1：Kashpureff 攻击，1997

- **历史背景： 90年代域名的战争——InterNIC 与 AlterNIC的冲突**
  - **攻击方案：**直接从**权威服务器处**回复虚假响应，解析器相信并**缓存所有回复**的资源记录
  - **漏洞成因：缺乏数据验证**



攻击者
客户端

Step1: Recursive query for
www.alternic.net/A

Step 2: Iterative query for
www.alternic.net/A

Step 3: Response including bogus
internic.net/NS RR

ISP resolver

Cache
InterNIC NS 1.2.3.4
www.internic.net A 5.6.7.8

Step 4:
Recursive query for
www.internic.net/A

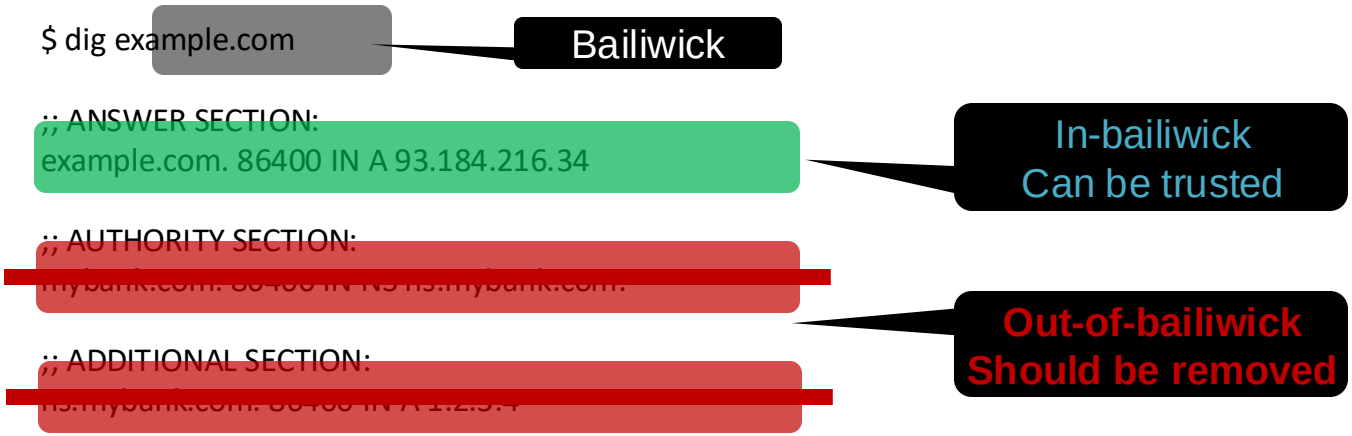
Step 5:Bogus Response
www.internic.net A 5.6.7.8

ALTERNIC.NET
alternic.nic

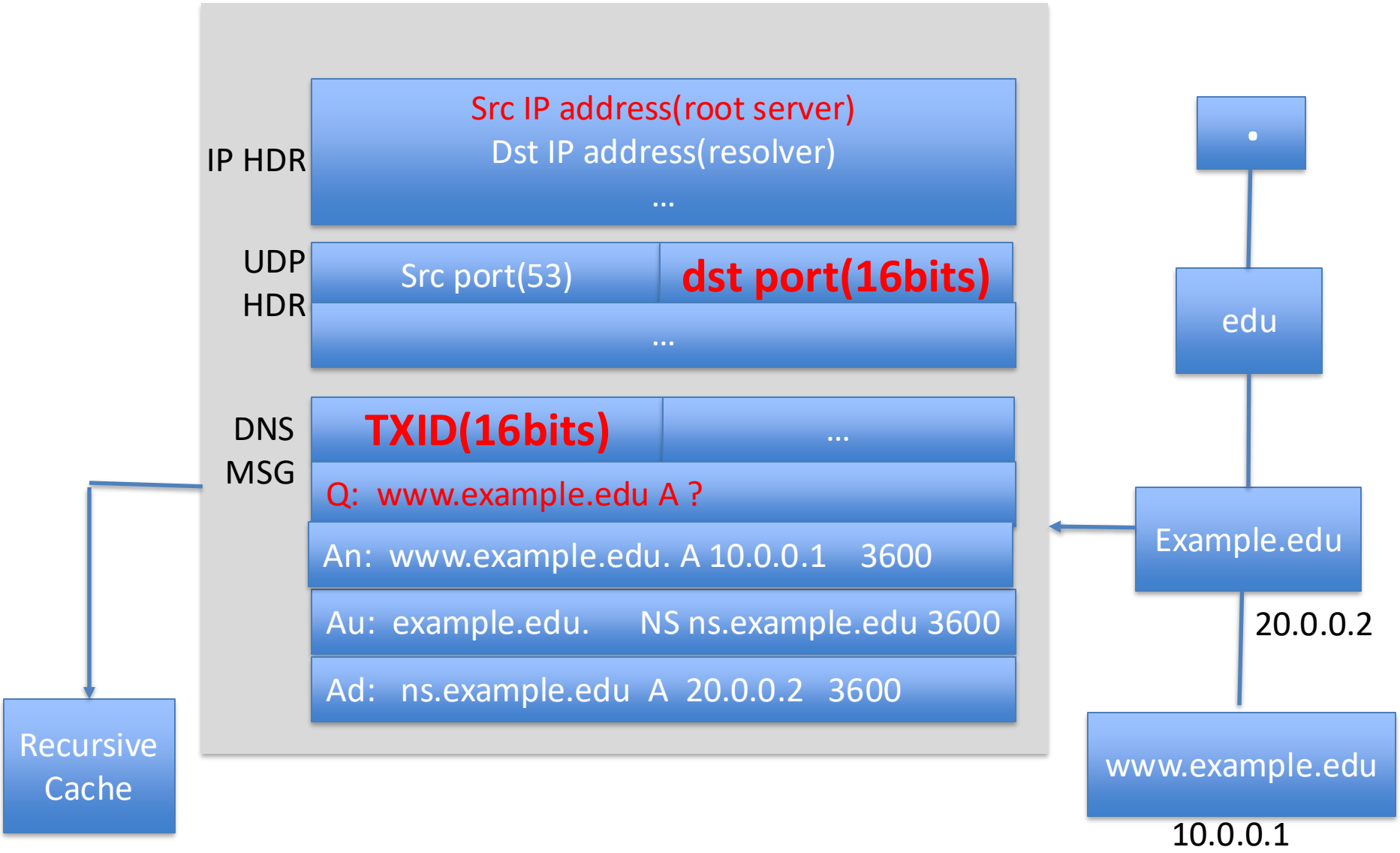
攻击者控制的
服务器

# 防御1：域名辖区原则（Bailiwick Rules），1997

- **RFC2181：Clarifications to the DNS Specification**
  **具体策略：在接收响应回复时对其合法性进行检查**
  - **辖区原则**：回复资源记录的域名属于对应权威域名服务器**管辖区域的子域名**
  - **执行方式**：**符合辖区原则即被缓存**，否则被移除

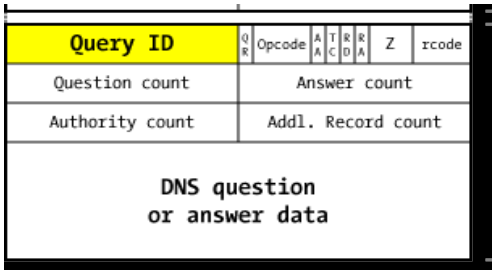


# DNS reply from Authoritative Server



# 攻击2：Dan Kaminsky， 2008

- **Dan Kaminsky 攻击，2008, Blackhat**
  - **漏洞成因**：仅依靠 16-bit 的 TXID 防御

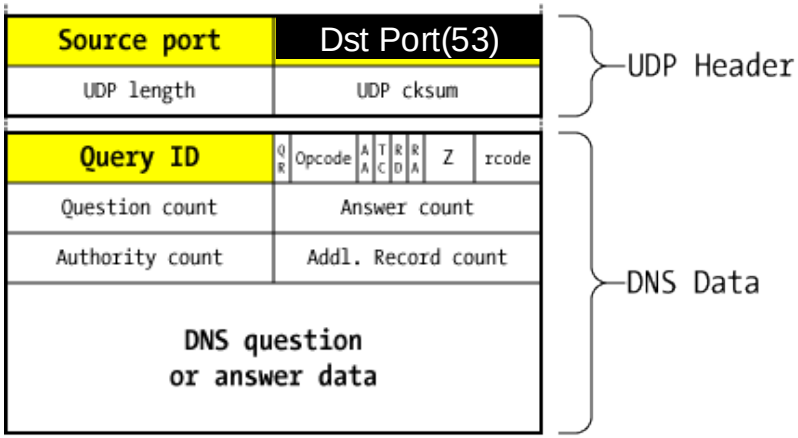



# The Flaw (1999 Edition)

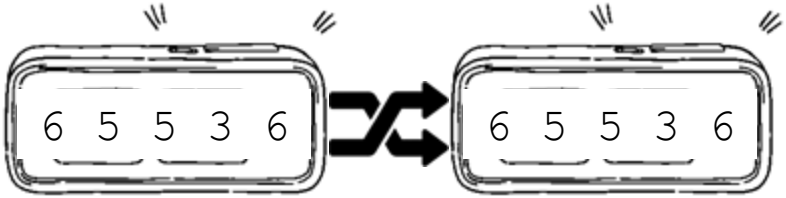
- 1999: DJB says 16 bit transaction ID's on queries aren't enough – attacker can brute force and guess responses
  - DNS community responds: "There has to be a query waiting for a response, for an attacker to guess a response. The TTL – Time To Live – limits how rapidly an attacker can force new queries awaiting responses. So if the TTL is one day, an attack will take years!
    - This *almost* became an RFC – "Forgery Resilience" – advocating long TTL's

# 防御2：DNS 查询源端口随机化

- **用于抵御 Kaminsky 攻击**
  - **具体策略：提升校验字段熵值空间的大小**，增加猜解的难度
  - **熵值空间：16位源端口** x 16位 TXID = 32位校验值
  - **抵御效果：**32位空间使得几乎无法暴力猜解




*DNS packet on the wire*



基于侧信道的DNS缓存污染， CCS 2020，杰出论文奖

# DNS Cache Poisoning Attack Side Channel Reloaded

Keyu Man, Zhiyun Qian, Zhongjie Wang, Xiaofeng Zheng, Youjun Huang, Haixin Duan

UC RIVERSIDE

清華大學 Tsinghua University

奇安信 QI-ANXIN

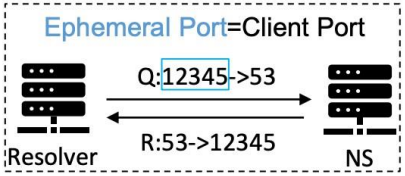
# 攻击的影响

- 所有层次的DNS解析器
  - 终端
  - 递归服务器
  - DNS转发服务器
- 全球开放递归34%可被攻击
- 知名的公共DNS服务12/14可被攻击

| | |
|---|---|
| Google | 8.8.8.8 |
| Cloudflare | 1.1.1.1 |
| OpenDNS | 208.67.222.222 |
| Comodo | 8.26.56.26 |
| Dyn | 216.146.35.35 |
| Quad9 | 9.9.9.9 |
| AdGuard | 176.103.130.130 |
| CleanBrowsing | 185.228.168.168 |
| Neustar | 156.154.70.1 |
| Yandex | 77.88.8.1 |
| Baidu DNS | 180.76.76.76 |
| 114 DNS | 114.114.114.114 |
| Tencent DNS | 119.29.29.29 |
| Ali DNS | 223.5.5.5 |

# DNS Cache Poisoning

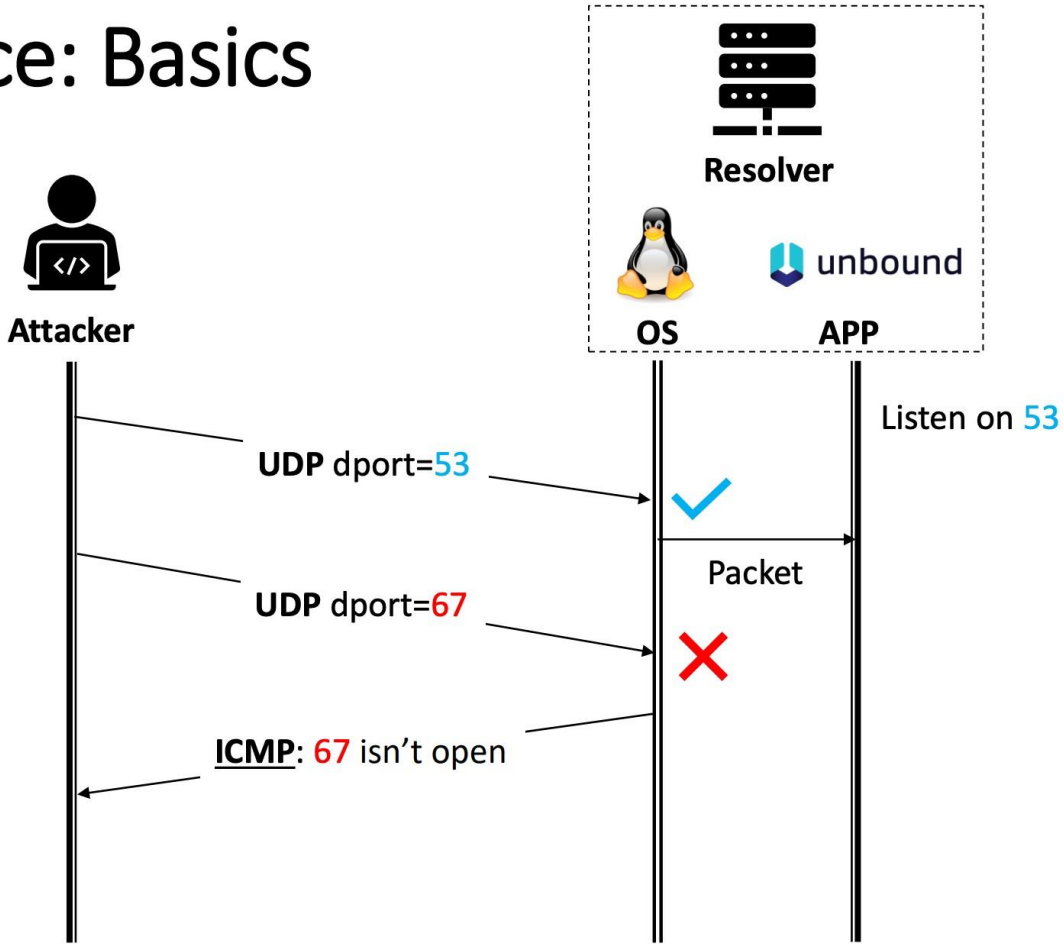

| | | |
|---|---|---|
| IP Layer | **Src:** 5.6.7.8 | |
| | **Dst:** *(resolver)* | |
| UDP Layer | **Src Port:** 53 | **Dst Port:** |
| DNS Layer | **TxID:** | |
| | **Question:** www.bank.com A ? | |
| | **Answer:** www.bank.com A 6.6.6.6, TTL=**99999** | |



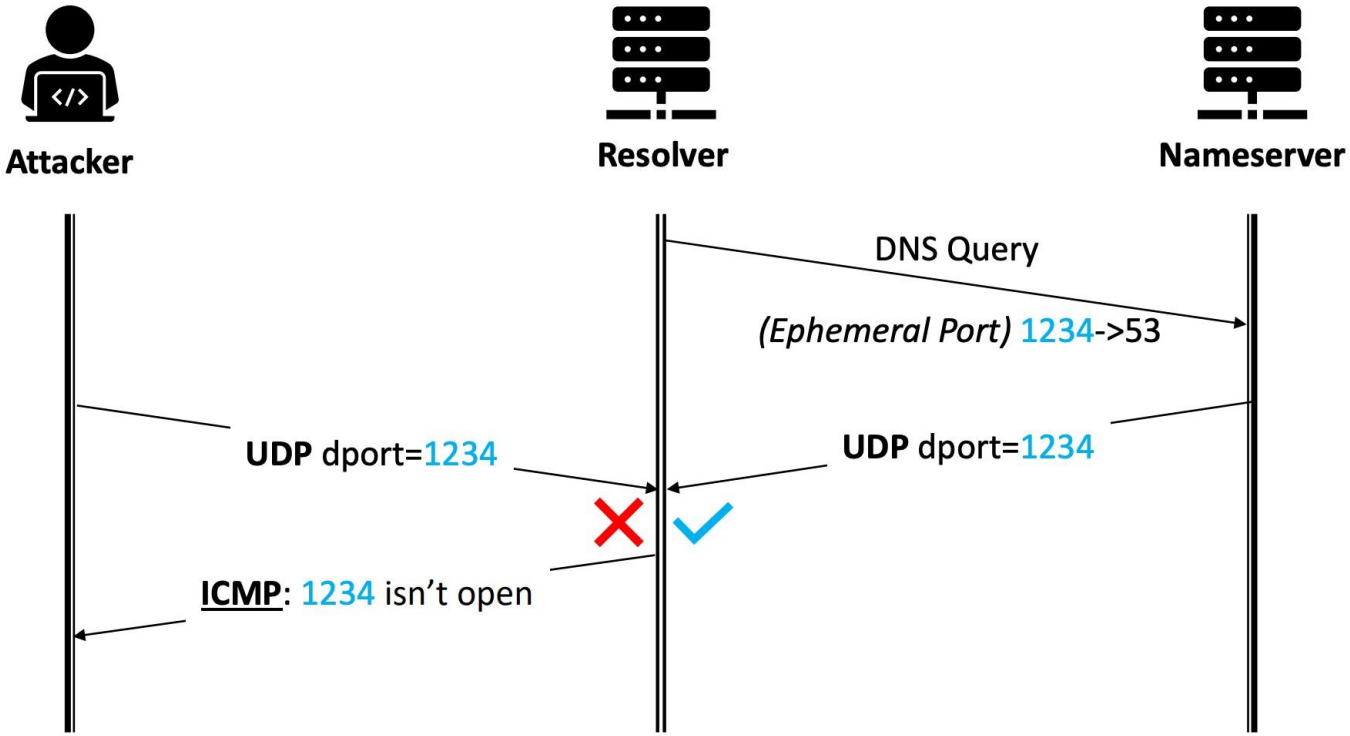

Traditional: $2^{16} \times 2^{16} = 2^{32}$ (Impossible in short time)

如果我们能够猜出 DNS 查询的源端口号呢？

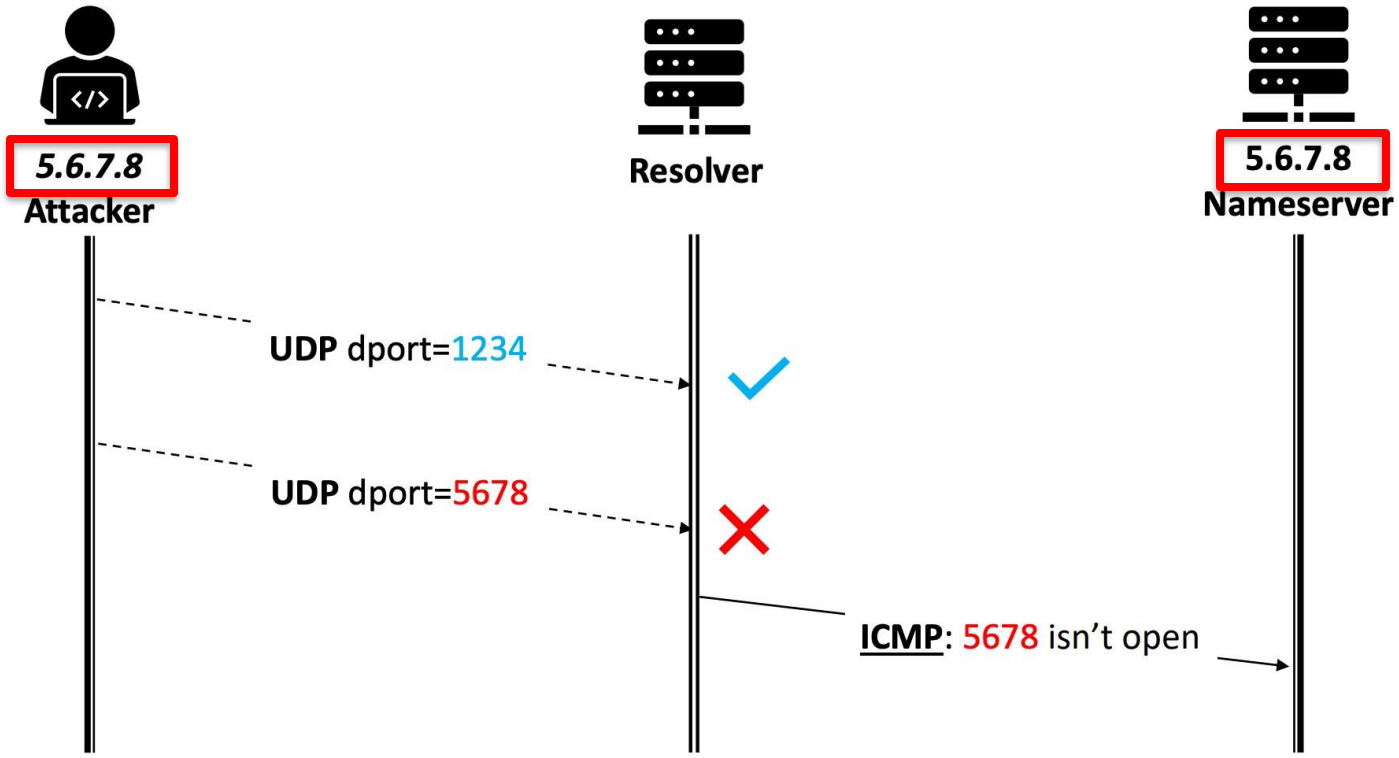
# Port Inference: Basics



# Port Inference: Ephemeral Ports

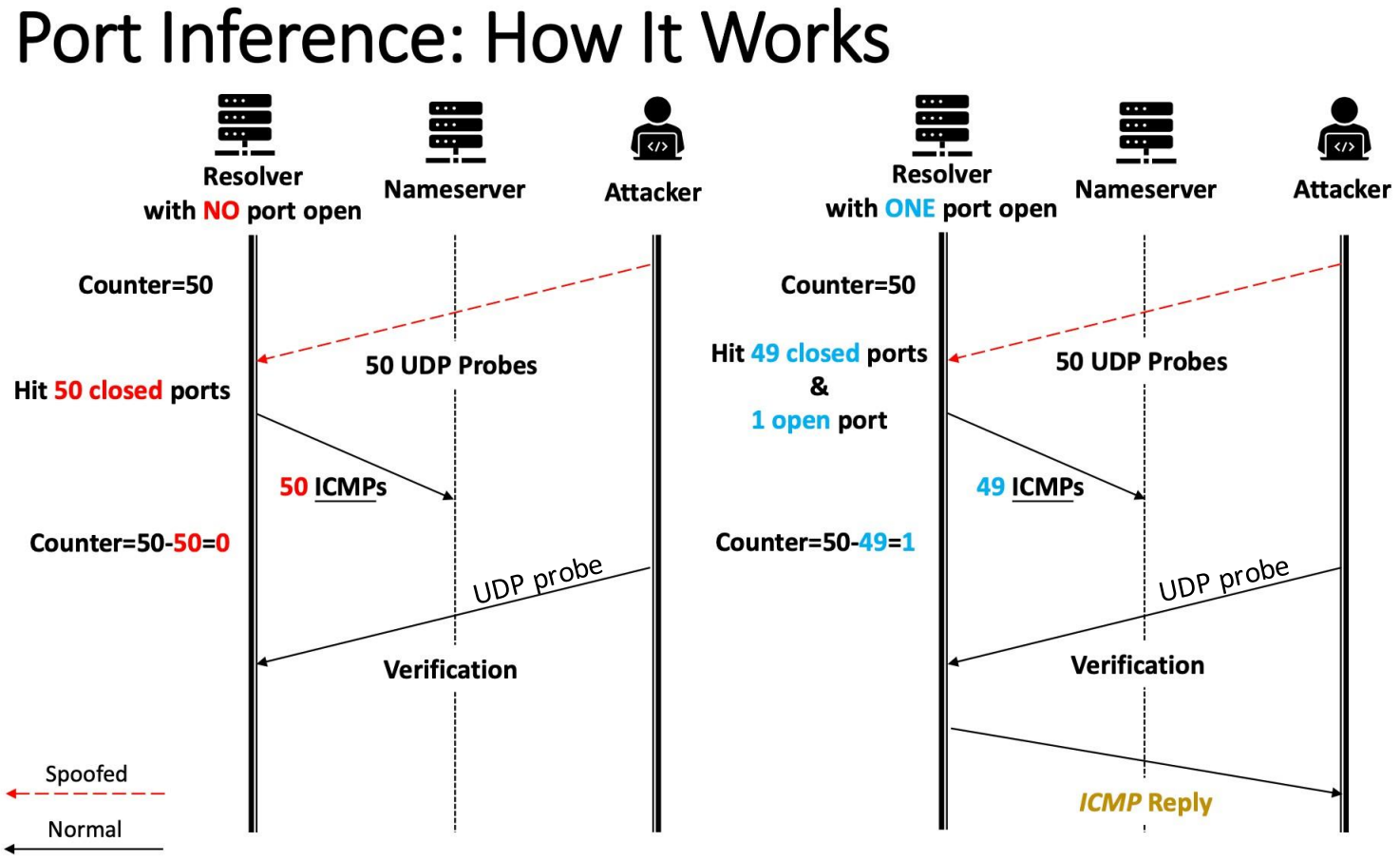


# Port Inference: IP Spoofing



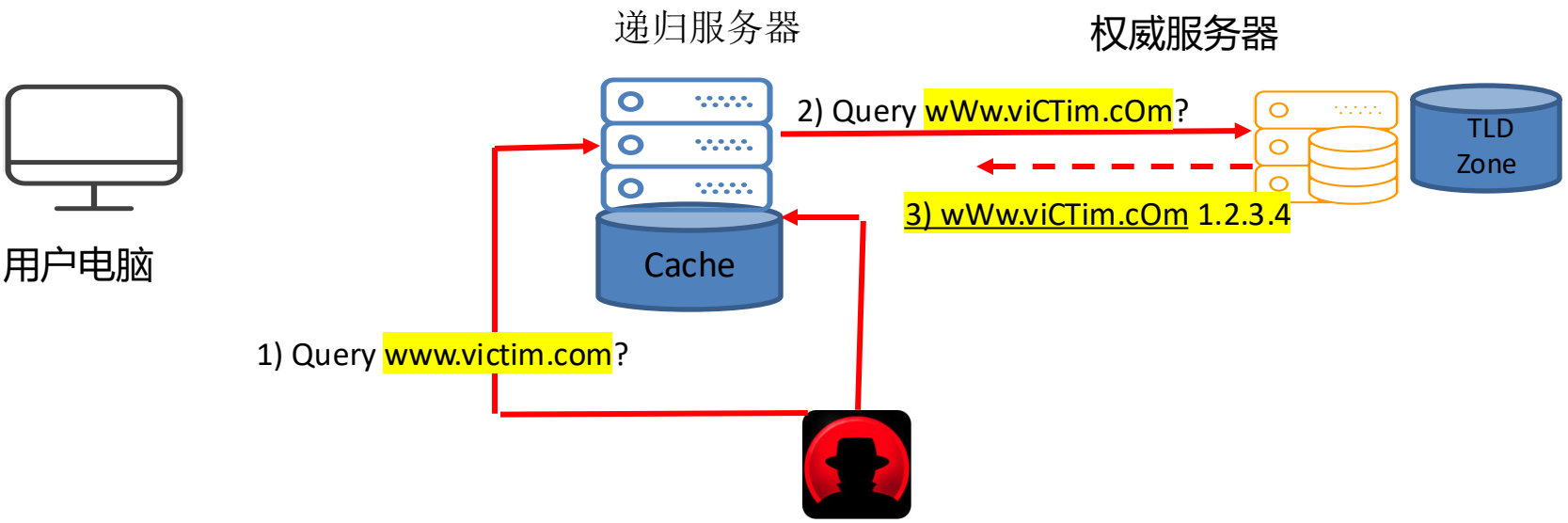

ICMP Global Rate Limit: 50 ICMPs / 50 ms
- Limit sending rate
- Shared by all IPs

# 利用OS协议栈侧信道猜测sPort，使缓存污染成功率恢复$2^{16}$



# 0x20 编码：不改变协议，增加攻击难度

- 权威服务器对查询域名的大小写是不敏感的；在DNS响应中**拷贝查询中的名字**
- 递归服务器对发出去的DNS查询的大小写随机编码
- Off path攻击者必须猜中大小写，增加的复杂度 2^length(qname)




[1] D. Dagon, M. Antonakakis, P. Vixie, T. Jinmei, and W. Lee, “Increased DNS forgery resistance through 0x20-bit encoding: security via leet queries,” CCS , 2008.

# Increased DNS Forgery Resistance Through 0x20-Bit Encoding

SecURItY viA LeET QueRieS

To efficiently encode a query, we propose a simple algorithm. Figure 5 illustrates the following steps:

1. As an input, a domain name input arrives: either an answer from a server, or a query from a stub resolver. Figure 5 shows the arrival of `IBM.com` as a query string.

2. First, one transforms the query field into a canonical format, e.g., all lowercase.

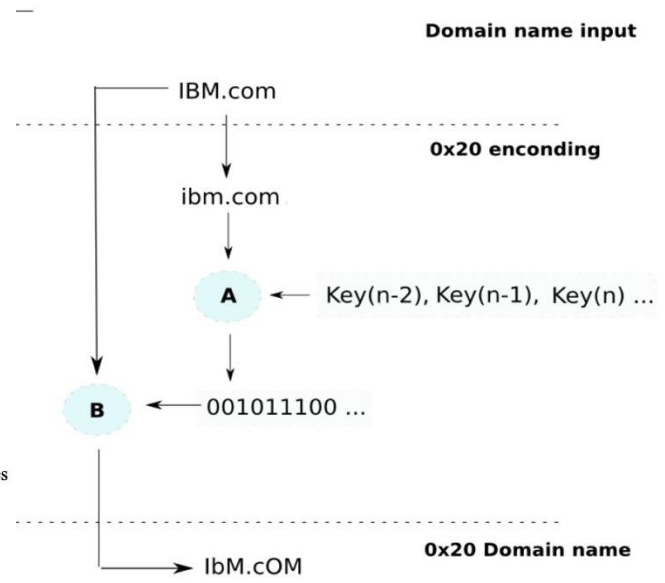
3. Second, one uses a chosen encryption scheme to encrypt the canonical query, e.g., perhaps with AES [23], and a key shared by all queries on the recursive server. This is illustrated as step A in Figure 5. This step could equivalently use a small number of keys, one for a given time epoch. (Key management is beyond the scope of this algorithm, but briefly noted below.)

4. Since the resulting cipher block is longer than the original query in terms of bytes, bits are read in sequential fashion from the cipher block. The query field, called `buff` is read one byte at a time. Step B in Figure 5 shows the encoding of all "0x20 capable" characters (i.e., `A-Za-z`.) In such a case, one reads the next bit $j$ from the ciphered block, and:

   (a) if the $j$th bit is 0, make the $i$ query character upper case (i.e., `buff[i] |= 0x20`).

   (b) if the $j$th bit is 1, make the $i$ query character lower case (i.e., `buff[i] &= 0x20`).

5. This produces a 0x20-encoded domain name, as shown in the final segment of Figure 5. This can be sent to an authority server. Likewise, it can be used to verify the query field returned by an authority server.




(a) if the $j$th bit is 0, make the $i$ query character upper case (i.e., `buff[i] |= 0x20`).

(b) if the $j$th bit is 1, make the $i$ query character lower case (i.e., `buff[i] &= 0x20`).

# 三个随机化之后： sPort, TXID, 0x20

| Source port | Destination port |
|---|---|
| UDP length | UDP cksum |

UDP Header

| Query ID | QR | Opcode | AA | TC | RD | RA | Z | rcode |
|---|---|---|---|---|---|---|---|---|
| Question count | Answer count | | | | | | | |
| Authority count | Addl. Record count | | | | | | | |

QUERY: wWw.GoOgLe.CoM

or answer data

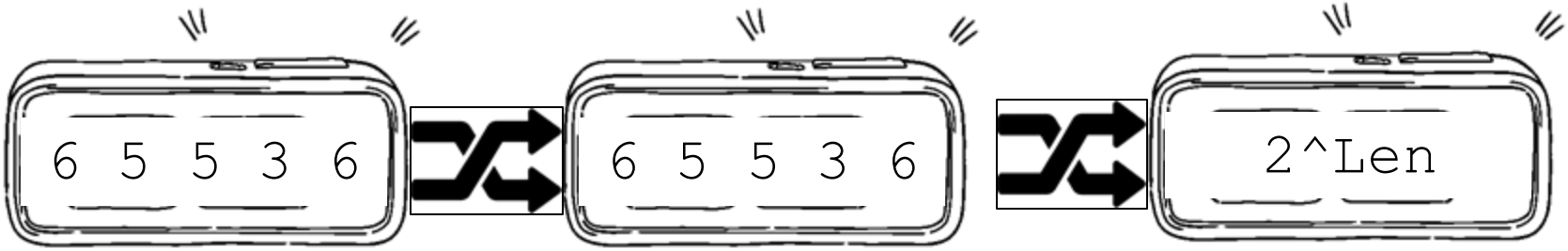
DNS Data

www.google.com

Len(www.google.com)=12

$2^{44}$ = 17592186044416

***DNS packet on the wire***




12306.CN ？

# DNS Cookie

https://datatracker.ietf.org/doc/html/draft-eastlake-dnsext-cookies-00

[Search] [txt|pdf|bibtex] [Tracker] [WG] [Email] [Nits]

Versions: 00 01 02 03 04 05
draft-ietf-dnsop-cookies

INTERNET-DRAFT — Donald E. Eastlake 3rd, Motorola Laboratories

Expires: December 2006 — June 2006

**Domain Name System (DNS) Cookies**

<draft-eastlake-dnsext-cookies-00.txt>

Status of This Document

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

This draft is intended to be become a Proposed Standard RFC. Distribution of this document is unlimited. Comments should be sent to the author or the DNSEXT working group mailing list <namedroppers@ops.ietf.org>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/lid-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Abstract

DNS cookies are a light-weight DNS transaction security mechanism. They provides limited protection to DNS servers and resolvers against a variety of increasingly common denial-of-service and cache poisoning attacks by off-path attackers.

https://datatracker.ietf.org/doc/html/rfc7873

[Search] [txt|html|pdf|bibtex] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

From: draft-ietf-dnsop-cookies-10 — Proposed Standard
Updated by: 9018

Internet Engineering Task Force (IETF) — D. Eastlake 3rd
Request for Comments: 7873 — Huawei
Category: Standards Track — M. Andrews
ISSN: 2070-1721 — ISC
May 2016

**Domain Name System (DNS) Cookies**

Abstract

DNS Cookies are a lightweight DNS transaction security mechanism that provides limited protection to DNS servers and clients against a variety of increasingly common denial-of-service and amplification/forgery or cache poisoning attacks by off-path attackers. DNS Cookies are tolerant of NAT, NAT-PT (Network Address Translation - Protocol Translation), and anycast and can be incrementally deployed. (Since DNS Cookies are only returned to the IP address from which they were originally received, they cannot be used to generally track Internet users.)

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

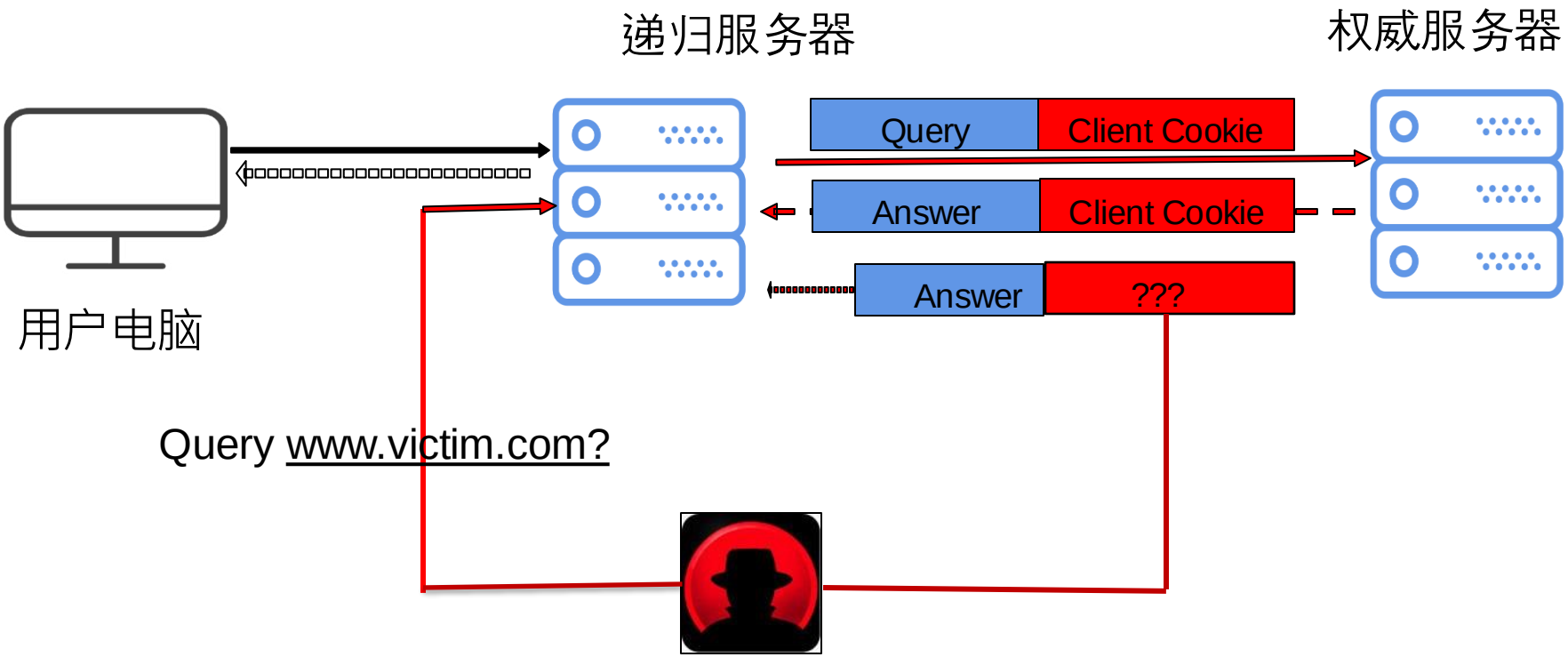
Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7873.

# DNS Cookies(RFC 7873), 2016

- Client Cookie防止缓存污染攻击
- 类似SYN Cookie，把不可伪造的随机值写入DNS query

- The Client Cookie :

HASH (Client IP, Server IP, secret)

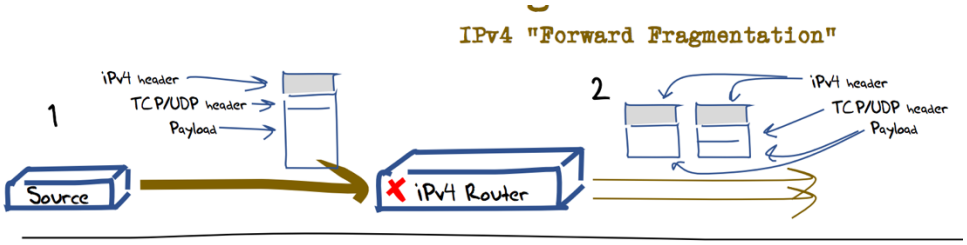


# 防范缓存污染的随机性措施

| 防缓存污染技术 | 世界 | 中国 |
| --- | --- | --- |
| 端口随机化 | 99.33% | 99.97% |
| TXID随机化 | 99.95% | 99.99% |
| 0x20编码 | 26.50% | 17.70% |
| DNS Cookies | 16.74% | 12.62% |

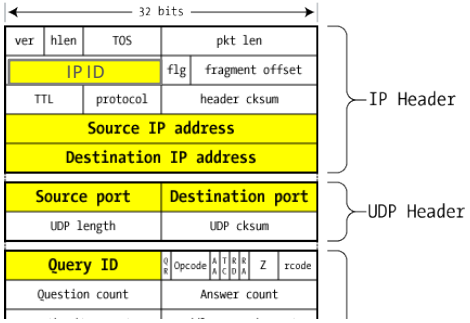
奇安信技术研究院司南系统2020年7月数据

# 预备知识：IP 分片（fragementation）

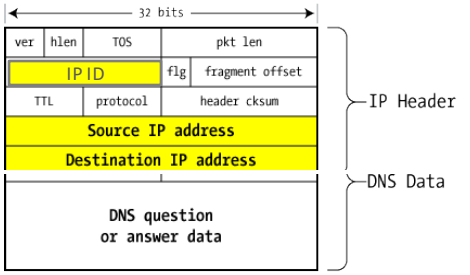



第二个分片中没有UDP Header、DNS Header

Frag1



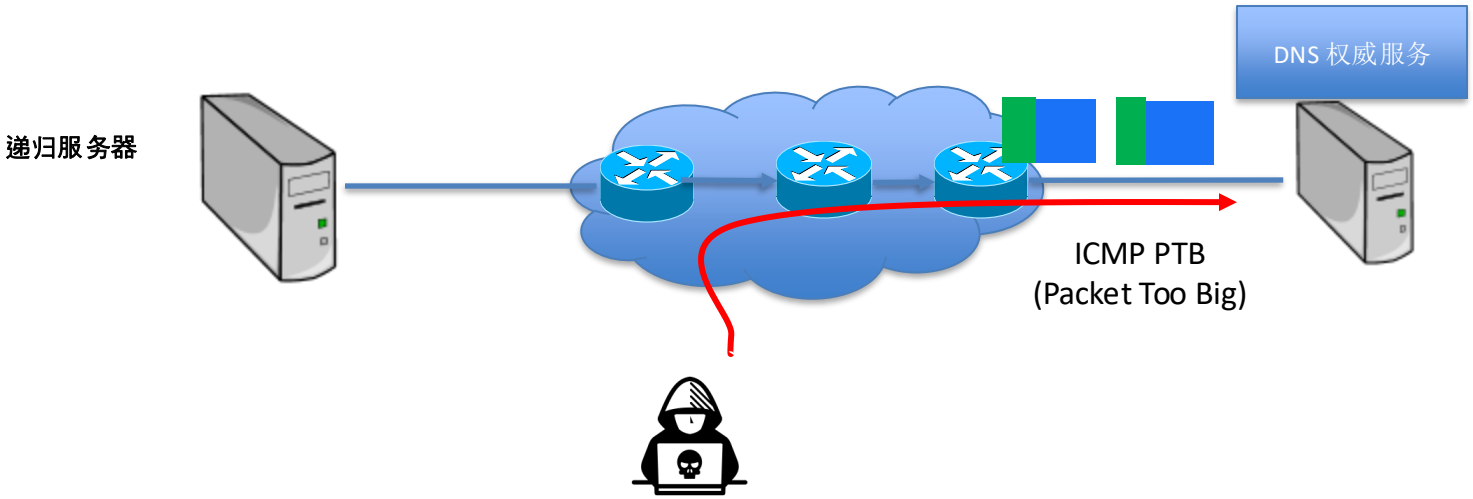

Frag2



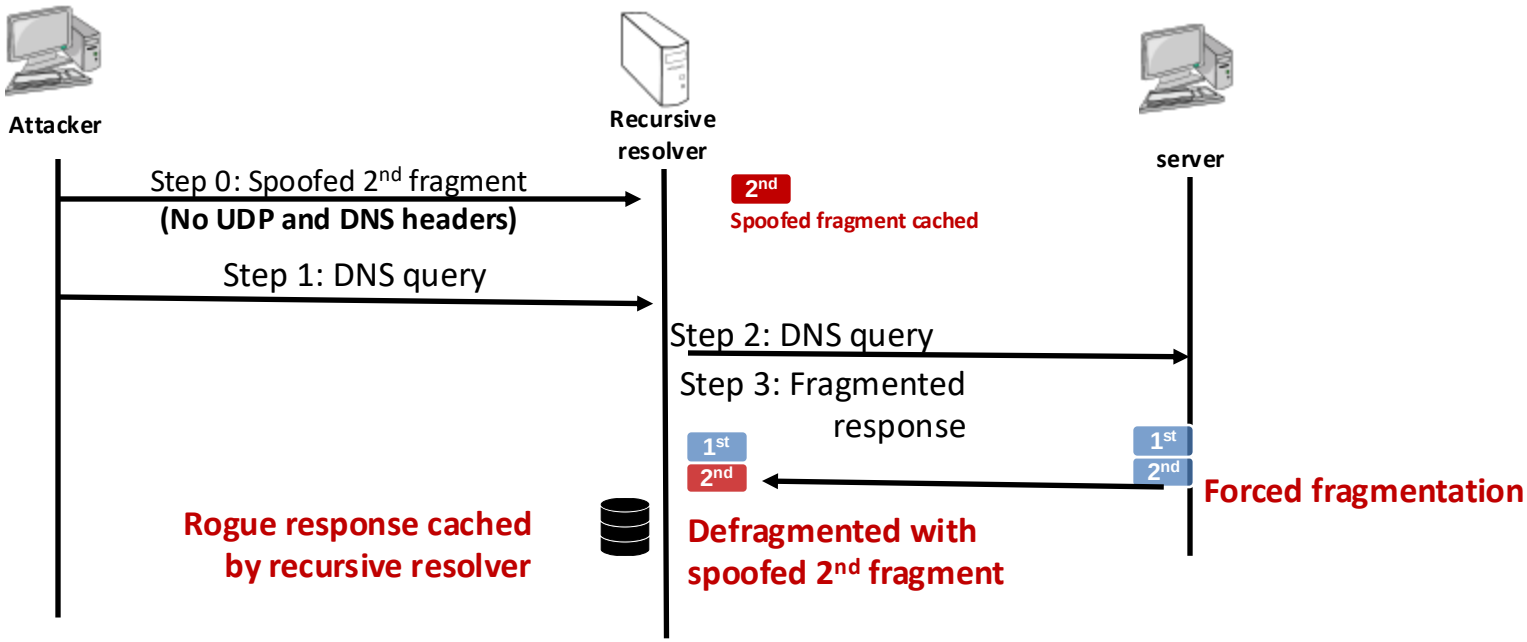

*DNS packet on the wire*

# 攻击3：基于分片的域名缓存污染

- **Herzberg，Shulrnan：Fragmentation Considered Poisonous， 2013**
  - **攻击方案**：利用**第二个分片不存在校验字段**的方式进行虚假回复的注入
  - **攻击效果**：解析器相信并缓存**分片重组后回复中的数据**
  - **漏洞成因**：**接受较小的分片数据包**



# 攻击3：基于分片的域名缓存污染，2013



# 防御：Linux 内核已经不允许小的DNS响应分片

- 2020年，Alexa Top 10万 的域名服务器中只有0.7%可以把MTU 降至528 Byte 以下
- 一般DNS响应 小于 512 Bytes，因此这种分片攻击不太可行了

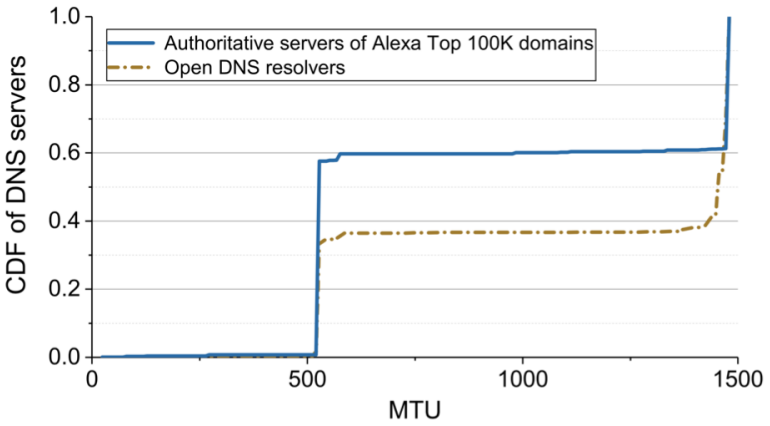
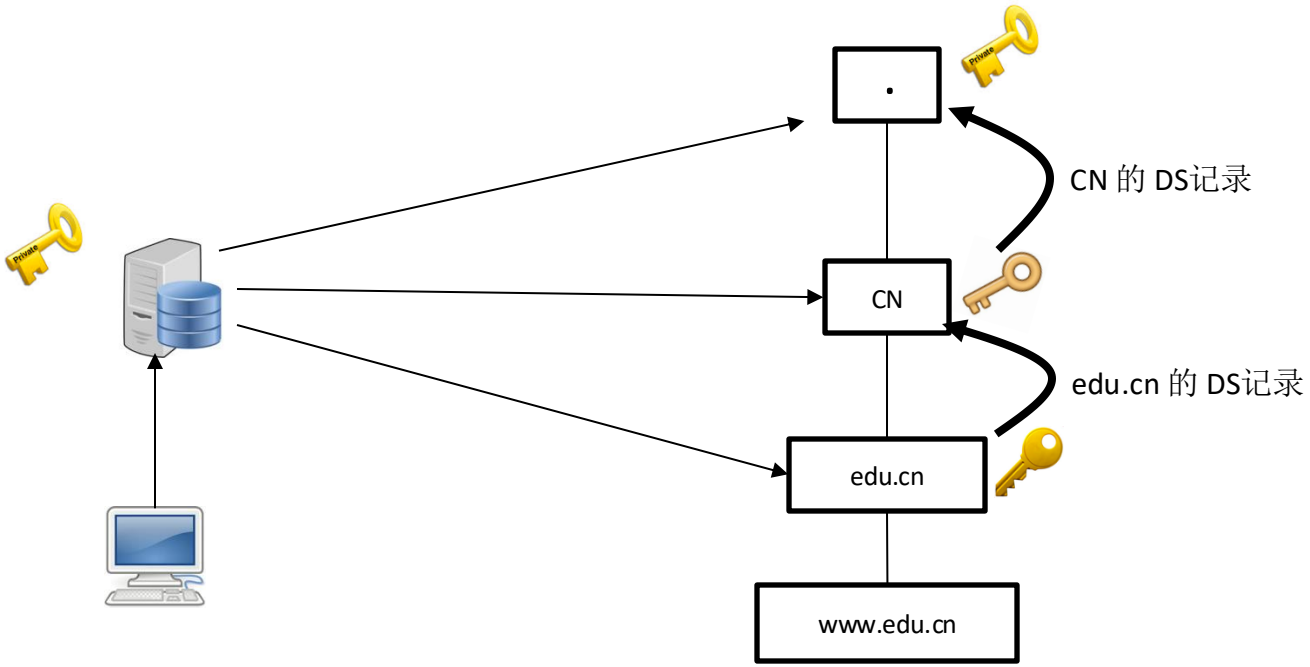



Figure 2: CDF of lowered MTU of a) authoritative servers of Alexa Top 100K domains, and b) 2M open DNS resolvers from an Internet-wide scan.

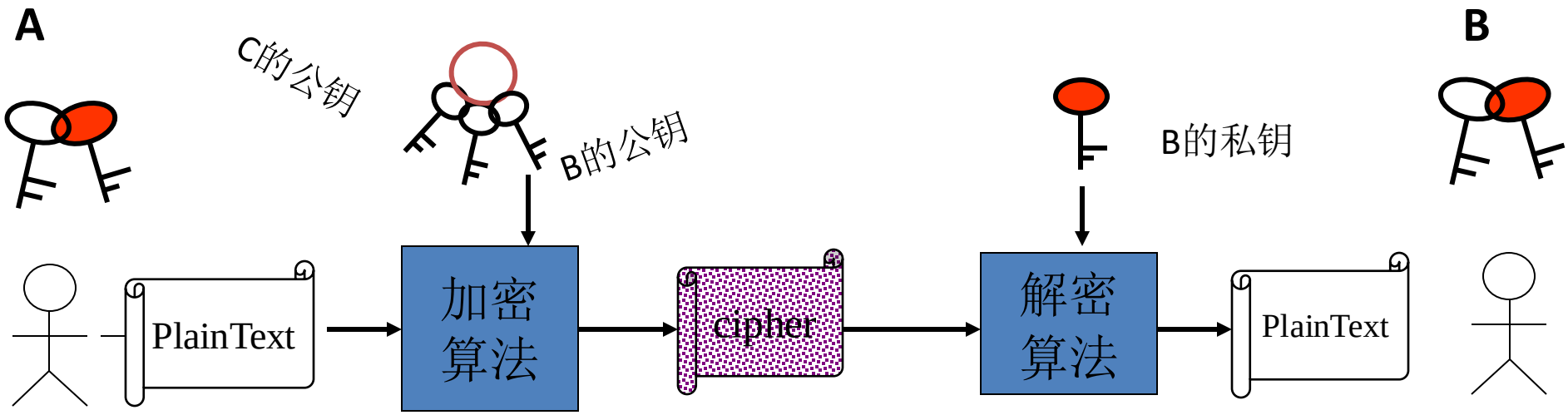
# DNSSEC:基于公钥算法的签名与验证

- Root 的公钥预置到所有客户端（递归解器）中
- Root 用自己的私钥对TLD的公钥（DS记录）签名
- 递归服务器可以验证TLD、SLD等签名的记录



# 基于公开密钥的加密

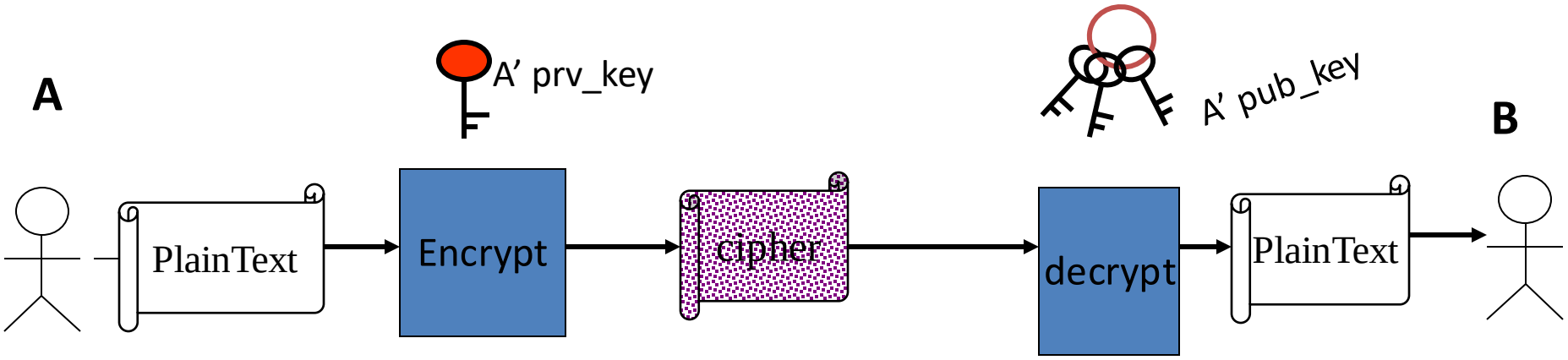
- 每个通信实体有一对密钥（公钥，私钥）。公钥公开，用于加密和验证签名，私钥保密，用作解密和签名
- A向B 发送消息，用B的公钥加密
- B收到密文后，用自己的私钥解密




任何人向B发送信息都可以使用同一个密钥(B的公钥)加密

没有其他人可以得到B 的私钥，所以只有B可以解密

# 数字签名与验证

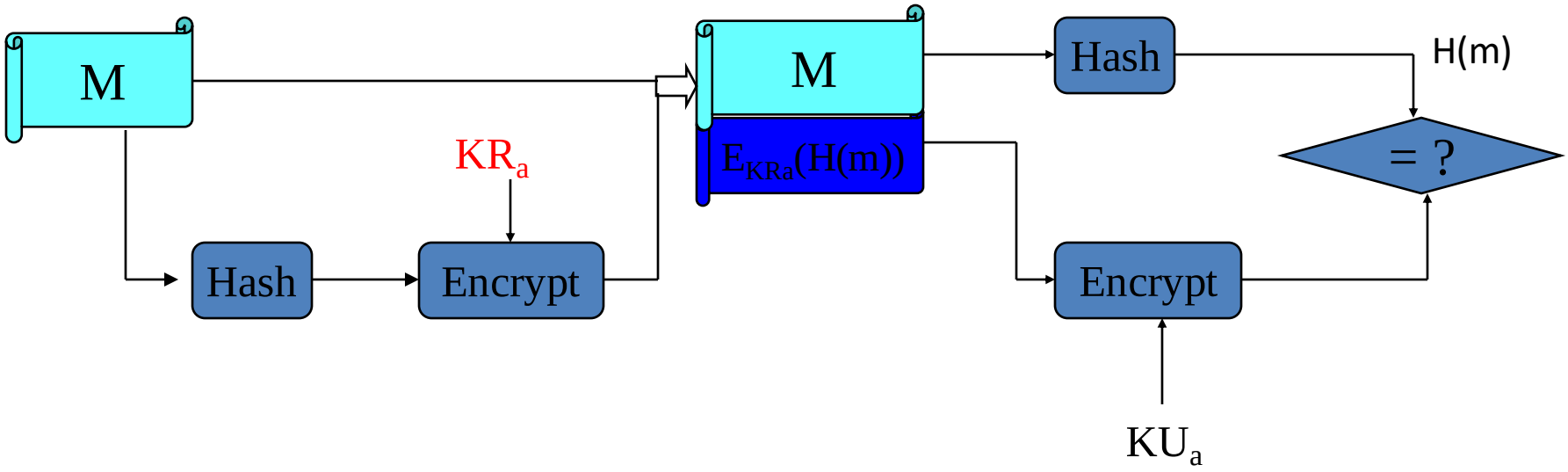



- A 用自己的私钥加密，即签名
- B 用签名方的公钥解密，即签名验证

# 先摘要（散列）再签名

公钥,私钥
A: ($KU_a$ $KR_a$), $KU_b$

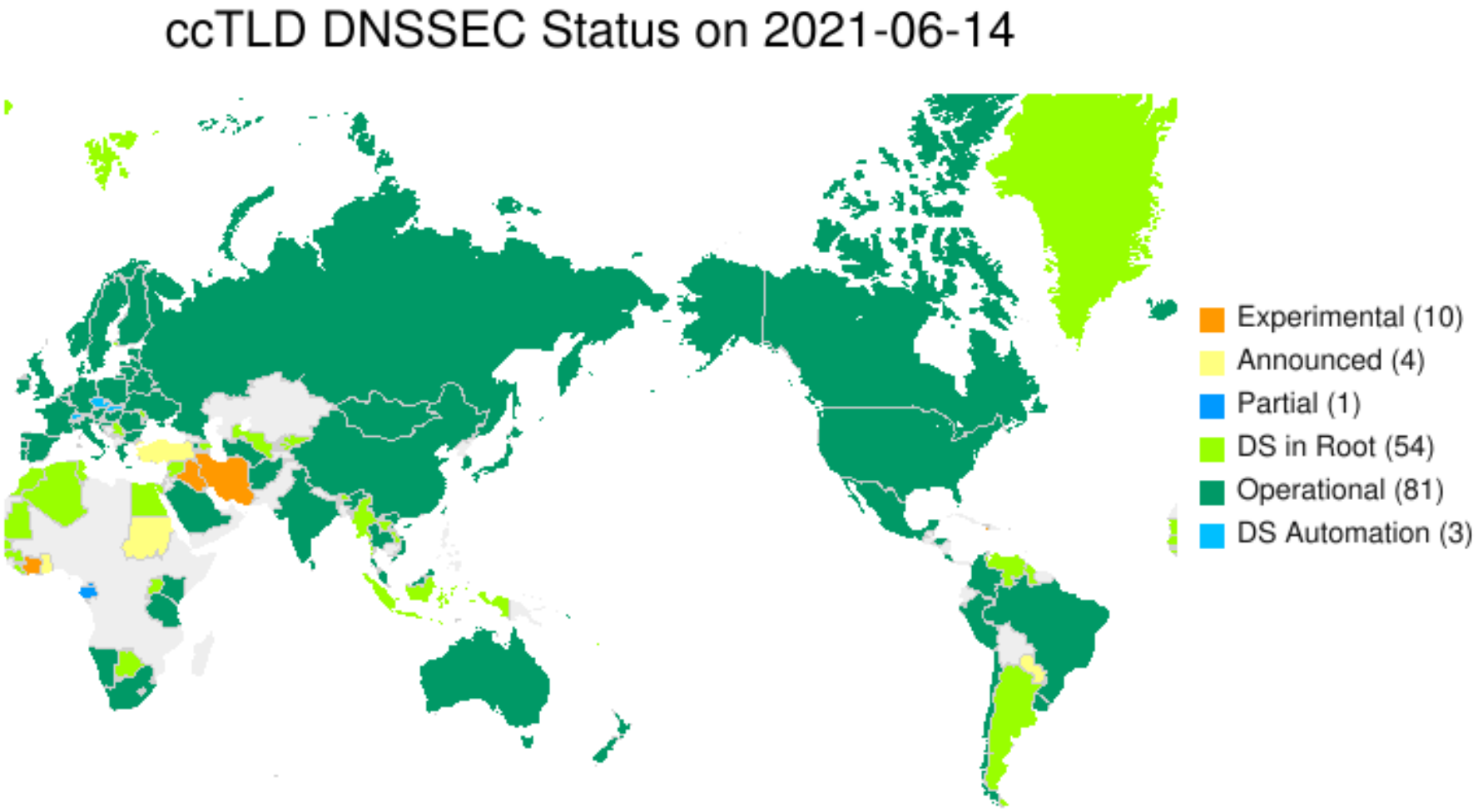
公钥,私钥
B: ($KU_b$ $KR_b$), $KR_a$



```
duanhx@MBP-abai ~ % dig  -t ds  edu.cn  +dnssec @a.dns.cn

; <<>> DiG 9.10.6 <<>> -t ds edu.cn +dnssec @a.dns.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41901
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;edu.cn.                                IN      DS

;; ANSWER SECTION:
edu.cn.                 86400   IN      DS      15397 8 1 CA602972D554DF57CC8322C18D9CF942FAC47430
edu.cn.                 86400   IN      DS      15397 8 2 3A6C89D32B3143D193521CE64389548821DA90F770AB09ECD9C8680B 2F4848B5
edu.cn.                 86400   IN      RRSIG   DS 8 2 86400 20221021153426 20220921144902 38388 cn. E2iFNCYhC8Hj4hWCZLm23wgP
4HgCl2LCMLKrbFXKF xNsv//e9wLXSbZTuyGUKbIA2mi2wWFffNfFbfuXEHhYsbPDSlGGvU/Ya 6oyZ6N29jTrrz3+GrWCzMNrPObehaFk0P5iYm7J9W5igTsgKH8
```

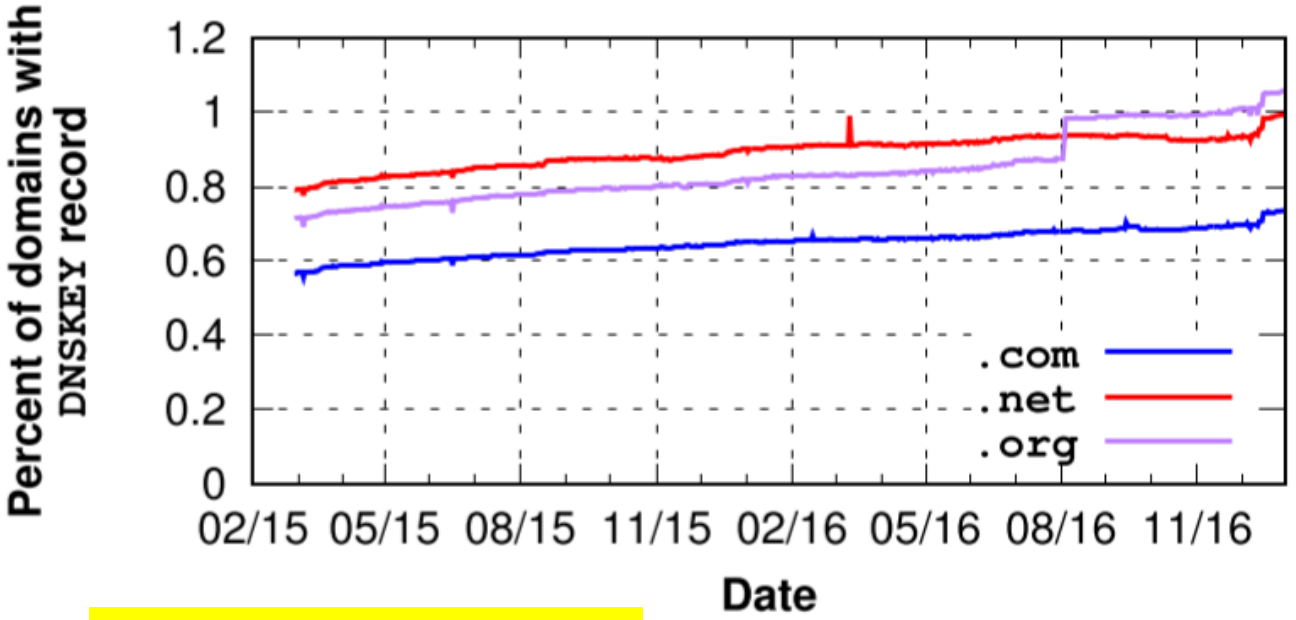
EDU.CN 把自己的公钥散列值（DS记录）上传至CN（a.dns.cn），由CN签名

```
duanhx@MBP-abai ~ % dig  -t ns edu.cn  +dnssec

; <<>> DiG 9.10.6 <<>> -t ns edu.cn +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58844
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;edu.cn.                                IN      NS

;; ANSWER SECTION:
edu.cn.                 13091   IN      NS      ns2.cernet.net.
edu.cn.                 13091   IN      NS      dns2.edu.cn.
edu.cn.                 13091   IN      NS      ns5.cernet.net.
edu.cn.                 13091   IN      NS      dns.edu.cn.
edu.cn.                 13091   IN      NS      ns3.cernet.net.
edu.cn.                 13091   IN      NS      ns4.cernet.net.
edu.cn.                 172647  IN      RRSIG   NS 8 2 172800 20221017030949 20220917030525 21204 edu.cn. GRp/54t0/v5
6hflEMQP1jLBhjuMe7nwVK hVCIrLMdIOSbE93amSZWZtysrq2H4RcKAOAZ9flBv5KuOUFLymI7/VpO hdThlU3PjWQ+12HYFA7s3pnUOBCmX0f7luAtr
=
```




https://www.internetsociety.org/deploy360/dnssec/maps/

# DNSSEC签名的部署情况(<1%)

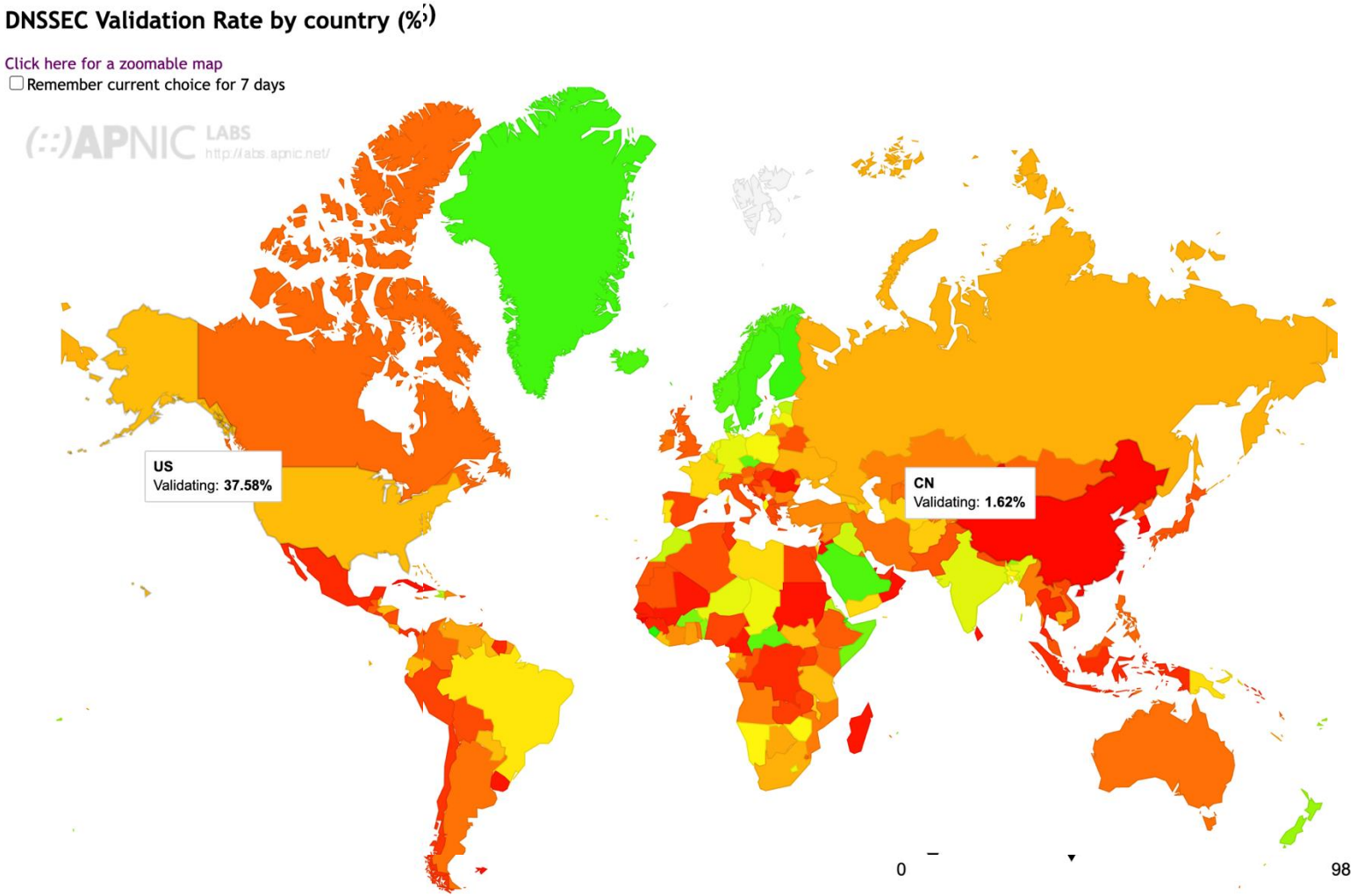



.com-0.6%
.org, .net – 1.0%

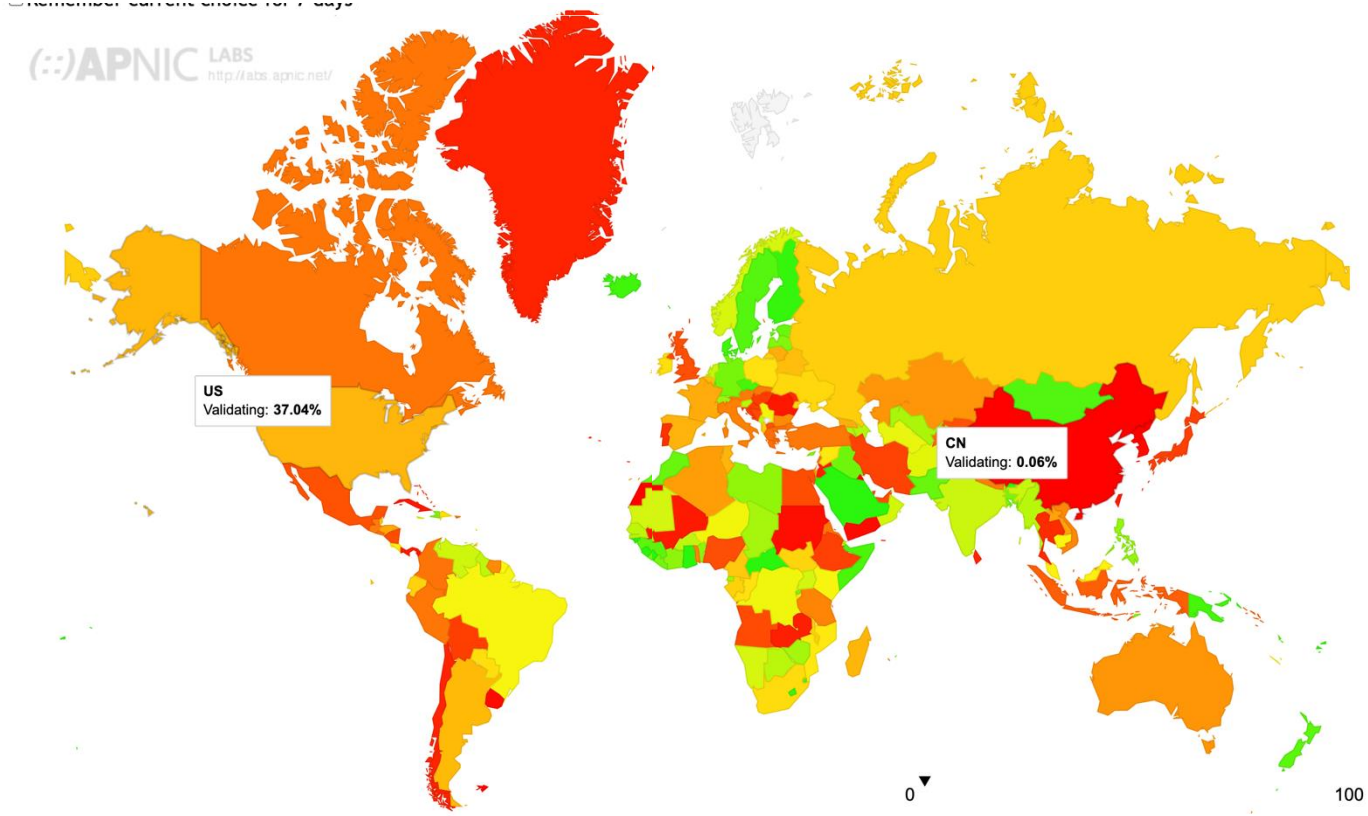
虽然很少，但仍在增长

Taejoong Chung , and etc. A Longitudinal, End-to-End View of the DNSSEC Ecosystem, USENIX Sec' 17

# 全球DNSSEC 验证的比例(2022)

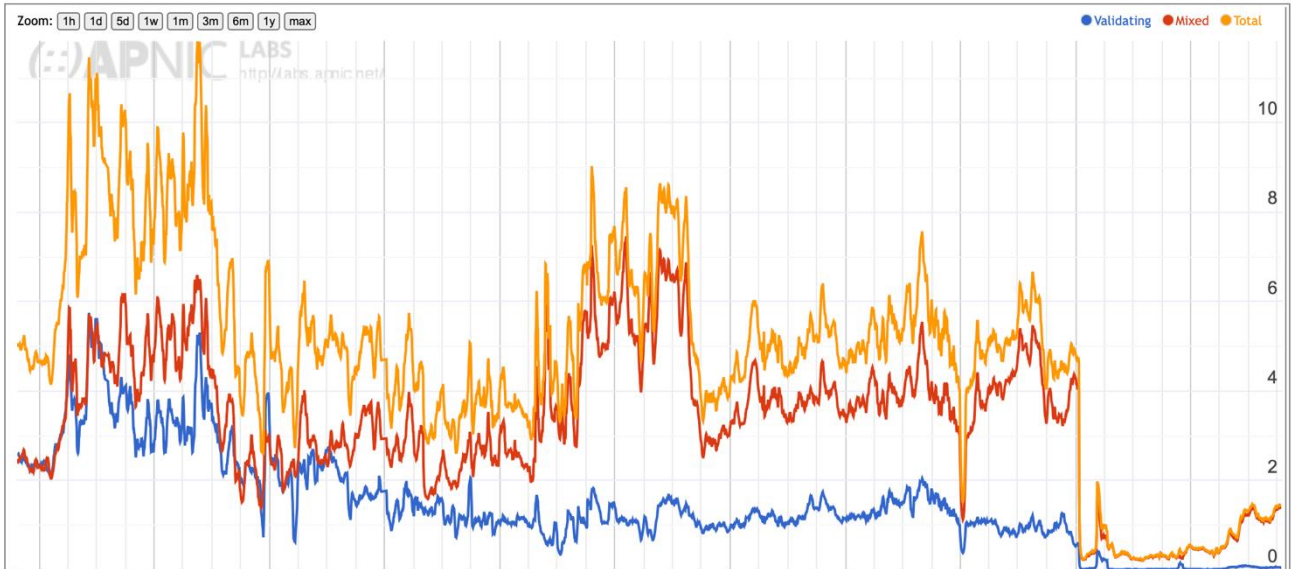



http://stats.labs.apnic.net/dnssec

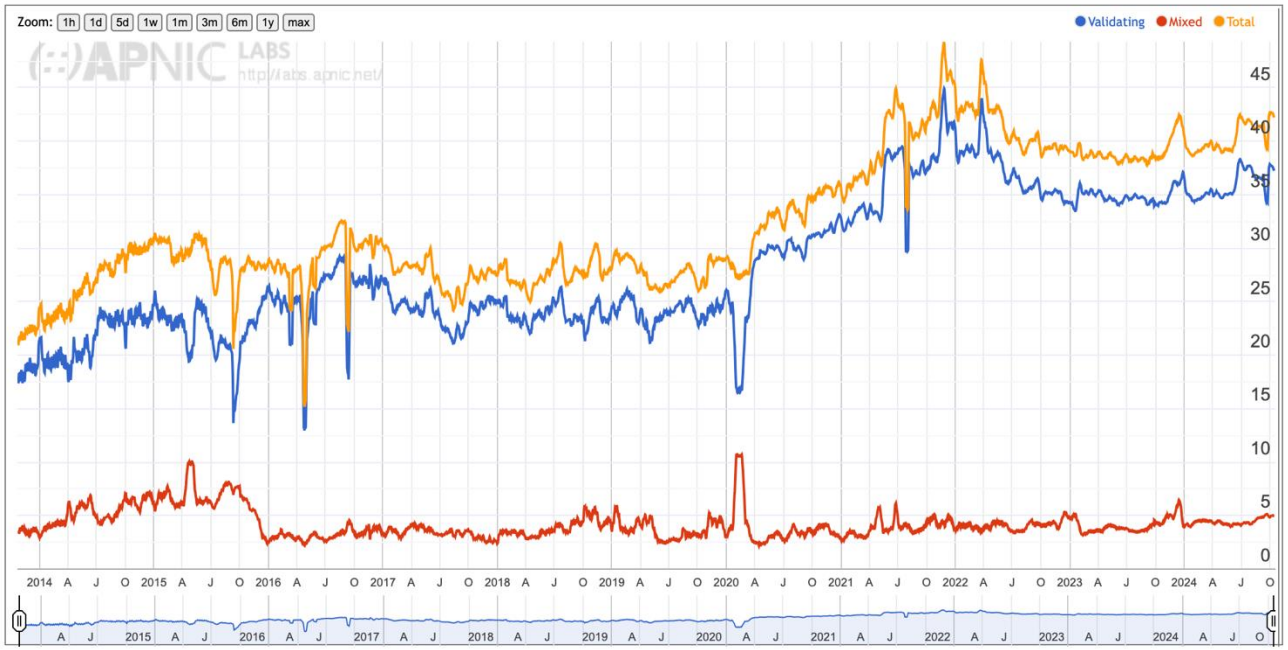



30 day average (15/09/2024 - 14/10/2024)

# Use of DNSSEC Validation for China (CN)




# Use of DNSSEC Validation for United States of America (US)



# 开放递归服务器分布及防污染措施（2020年8月）

- DNSSEC验证

| 配置问题 | 世界 | 中国 |
| --- | --- | --- |
| 支持DNSSEC | 38.14% | 13.88% |
| RRSIG过期 | 14.7% | 4.79% |
| RRSIG缺失 | 33.4% | 8.99% |
| RRSIG错误 | 13.72% | 4.79% |
| DS缺失 | 13.75% | 4.40% |
| DS错误 | 3.12% | 4.80% |
| 正确验证率 | 2.69% | 4.04% |

| 防缓存污染技术 | 世界 | 中国 |
| --- | --- | --- |
| 端口随机化 | 99.33% | 99.97% |
| TXID随机化 | 99.95% | 99.99% |
| 0x20编码 | 26.50% | 17.70% |
| DNS Cookies | 16.74% | 12.62% |

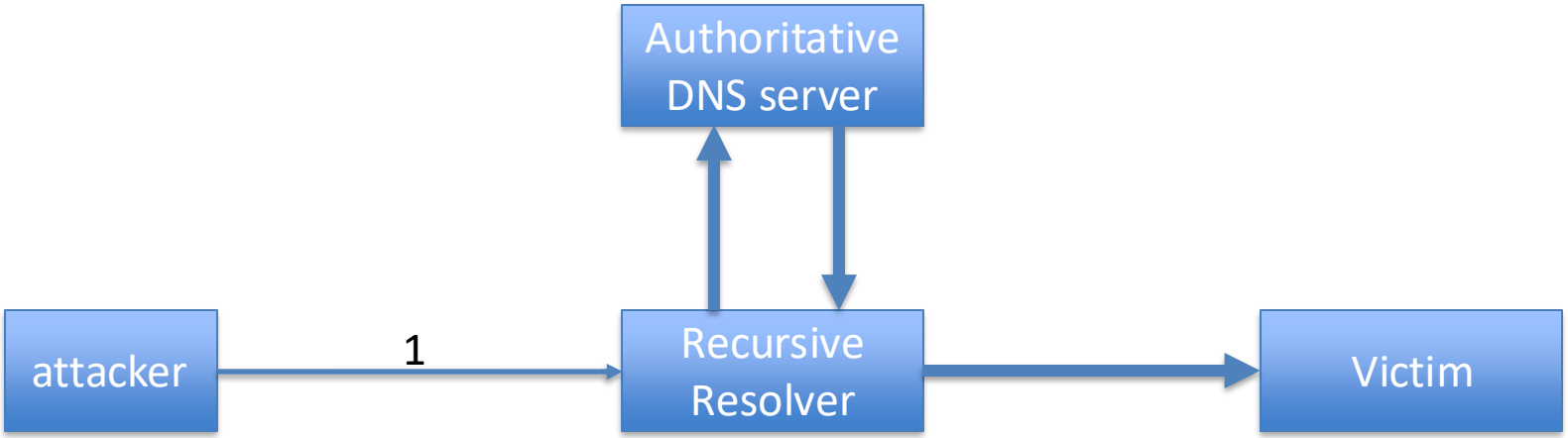
奇安信技术研究院司南系统2020年7月数据

# Content

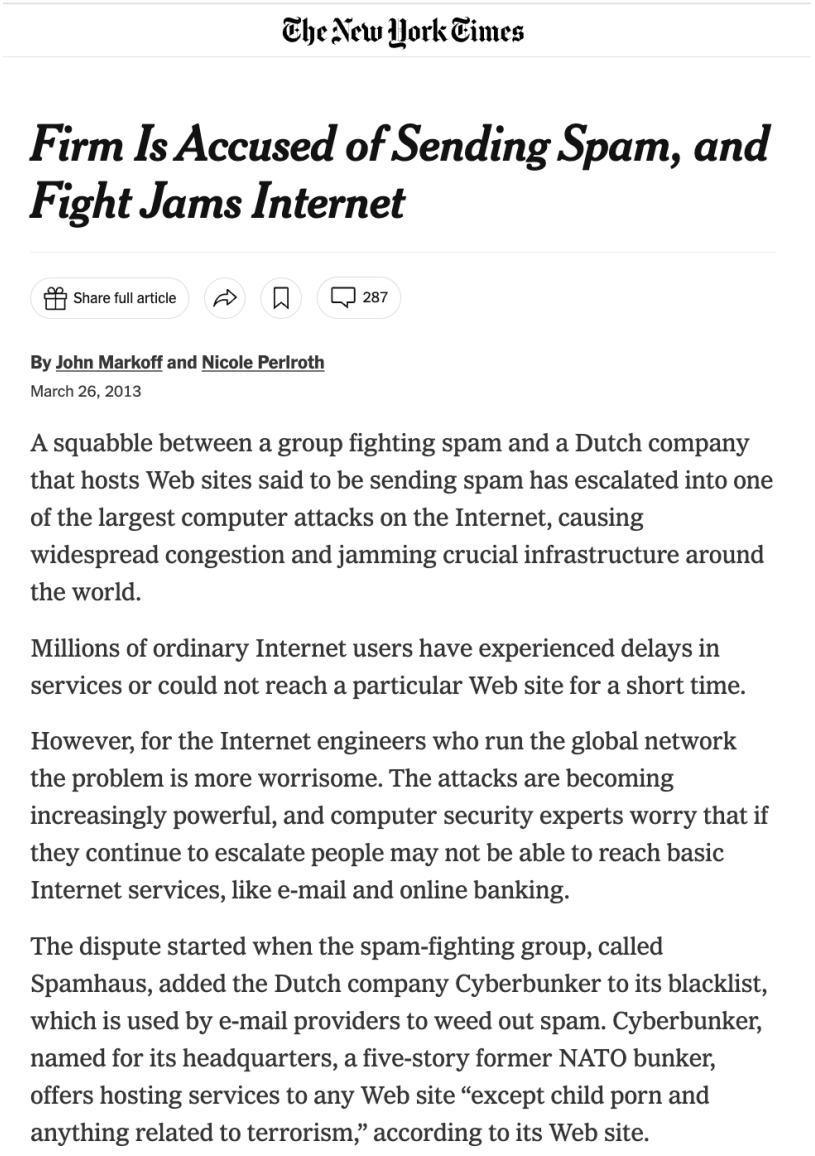
- DNS Incidents
- How DNS works
- DNS Root
- DNS Vulnerabilities and attack surface
- Root DNS  attacks
- Cache Poisoning attacks
- Reflective amplification DDoS attack, with DNS

# DNS反射放大攻击

- DNS over UDP(mostly), IP Spoofing is easy
- Amplification: Response > Query
- Huge number of DNS servers: 10M +



# 2013 年 Spamhaus 攻击



The New York Times

## *Firm Is Accused of Sending Spam, and Fight Jams Internet*

Share full article 287

By John Markoff and Nicole Perlroth
March 26, 2013

A squabble between a group fighting spam and a Dutch company that hosts Web sites said to be sending spam has escalated into one of the largest computer attacks on the Internet, causing widespread congestion and jamming crucial infrastructure around the world.

Millions of ordinary Internet users have experienced delays in services or could not reach a particular Web site for a short time.

However, for the Internet engineers who run the global network the problem is more worrisome. The attacks are becoming increasingly powerful, and computer security experts worry that if they continue to escalate people may not be able to reach basic Internet services, like e-mail and online banking.

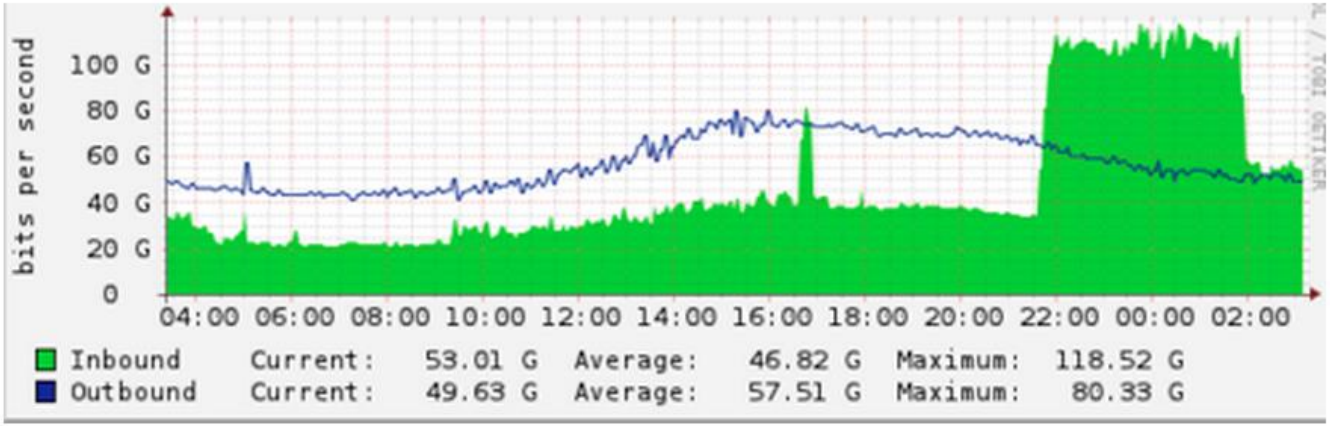
The dispute started when the spam-fighting group, called Spamhaus, added the Dutch company Cyberbunker to its blacklist, which is used by e-mail providers to weed out spam. Cyberbunker, named for its headquarters, a five-story former NATO bunker, offers hosting services to any Web site "except child porn and anything related to terrorism," according to its Web site.

- 2013 年针对 Spamhaus 的攻击也是一场规模空前的攻击，Spamhaus 是一家帮助打击垃圾邮件和垃圾邮件相关活动的组织。Spamhous 负责过滤多达 80% 的垃圾邮件，因而频频遭到希望垃圾邮件顺利到达目标收件人的恶意分子攻击。
- 这次攻击以 300 Gbps 的速度向 Spamhous 推送流量。攻击开始后，Spamhous 立即向 Cloudflare 寻求帮助并达成协议。Cloudflare DDoS 保护缓解了攻击。攻击者的回应是攻击特定互联网数据交换中心和带宽提供商，试图弄垮 Cloudflare。这次攻击没有达到目的，但确实给伦敦互联网交换中心（LINX）造成了重大问题。攻击的罪魁祸首原来是英国一名少年黑客，受雇发动此次 DDoS 攻击。
- https://www.cloudflare.com/zh-cn/learning/ddos/famous-ddos-attacks/

# DNS as Attacking Tools

blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho

attack is picking up again.



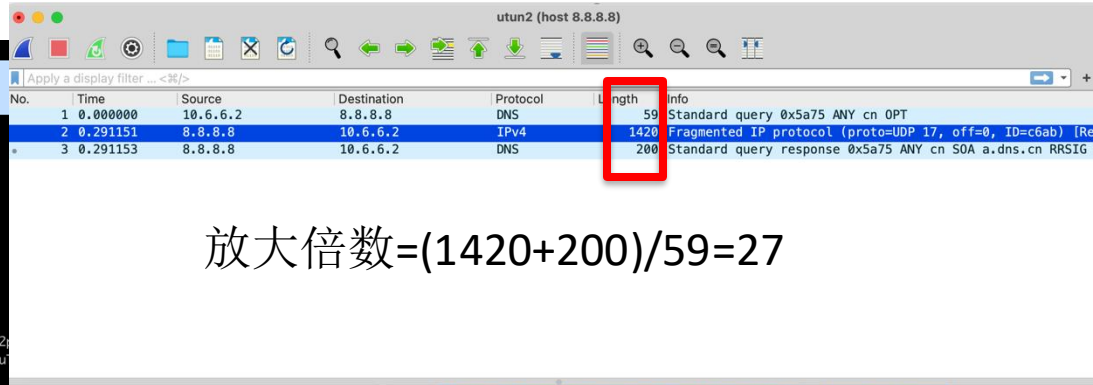

**How to Generate a 75Gbps DDoS**

The largest source of attack traffic against Spamhaus came from DNS reflection. I've written about these attacks before and in the last year they have become the source of the largest Layer 3 DDoS attacks we see (sometimes well exceeding 100Gbps). Open DNS resolvers are quickly becoming the scourge of the Internet and the size of these attacks will only continue to rise until all providers make a concerted effort to close them. (It also makes sense to implement BCP-38, but that's a topic for another post another time.)

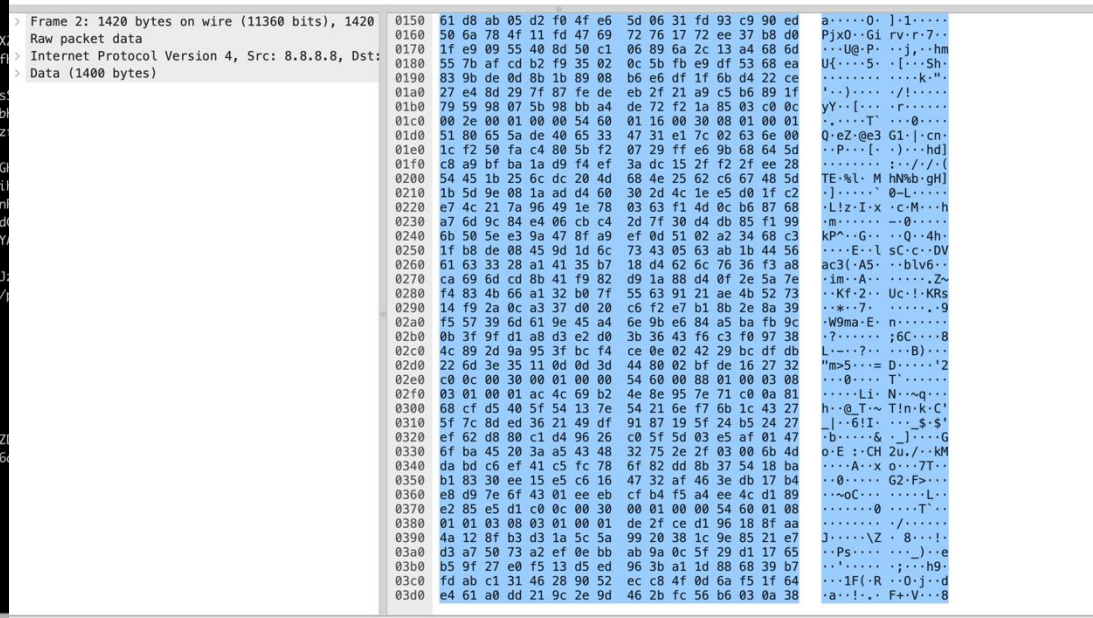
The basic technique of a DNS reflection attack is to send a request for a large DNS zone file with the source IP address spoofed to be the intended victim to a large number of open DNS resolvers. The resolvers then respond to the request, sending

# DNSSEC增大了DNS反射放大倍数

```
duanhx@MBP-abai ~ % dig +dnssec any cn. @8.8.8.8

; <<>> DiG 9.10.6 <<>> +dnssec any cn. @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23157
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 15, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;cn.                            IN      ANY

;; ANSWER SECTION:
cn.                     21600   IN      SOA     a.dns.cn. root.cnnic.cn. 2031477117 7200 3600 2419200 21600
cn.                     0       IN      RRSIG   NSEC3PARAM 8 1 0 20231120041912 20231021033617 38388 cn. VYnQWZ
jvgVvK3+S3oOGJ01EXOwlJc0fD/r3k0StlhnJOLG0 LirUyRNdutH77OGMQ27qQv/u4V4ZpVXruWmBOFJ8eUoT45Cs5xv6k8WC qykdmlje/bmu
0+UCrpw1D3hgZ4p5Fu3+2GqDVgN2CRtYSBo YHA=
cn.                     0       IN      NSEC3PARAM 1 0 10 AEF123AB
cn.                     21600   IN      RRSIG   DNSKEY 8 1 86400 20231120041912 20231021033617 38388 cn. WCjmcX
5RSOfckZLYdirBdLwT+ZdBjH9k8mQ7VBqeE8R/Udp cnYXcu43uNAf6QlVQI1QwQaJaiwTpGhtVXuvzbL5NQIMW/vp31No6oOb 3g2LG4kItubf
I0pf4f+3usvIanFtokfeVmYB1uYu6TecvIa hQM=
cn.                     21600   IN      RRSIG   DNSKEY 8 1 86400 20231120041912 20231021033617 57724 cn. HPJQ+s
mm2hkXcipv7oa2fTvOtwVL/Iv7ihURRslbNwgTWhO JWLGZ0hdG12eCBqt1GAwLUwe5dAfwudMIXqWSR54A2PxTQy2h2inbZyE 5AbLxC1/MNTb
5pHj6nvDVECojRowx+43ghFnR1sc0MFY6sb RFZhYzMooUE1txjUYmx2NvOoymltzYtB+YLZGojUDy5afvSDS2ahMrB/ VWORIa5LUnMU+SoMoz
LLoo59Vc5bWGeRaRum+aEpbr7nAs/ n9Go0+LQOzZD9sPwlzhMiS2alT+89M4OAkIpvN/bIm0+NRENDT1EgAK/ 3hYnMg==
cn.                     21600   IN      DNSKEY  256 3 8 AwEAAaxMabJOjpV+ccAKgWjP1UBfVBN+VCFu92scQydffI3tNiFJ35G
n72LYgMHUlibAX10D5a8BR2+6RSA6pUNIMnUuLwMAa03avcbv QcX8eG+C3Ys3VBi6sYMw7hXlxhZHMq9GPtsXtOjZfm9DAe7rz7T1pO5M 0YniI
cn.                     21600   IN      DNSKEY  257 3 8 AwEAAd4vztGWGI+qShKPs9MaXFqZIDgcnoUh59OnUHOi7w67q5oMXyn
g9RPV7ZY7oR2IaDm3/avBMUYokFLsyE8NavUfZORhoN0hnC6d Riv8VrYDCjj5VSh7kwk157mm3BxLn1XTs9Jys44bJ17fNxNjS4AGdUa9 4pOd
6dUtWp8jz9ffborCWvsXtp3AsEJs7eFAmOJIqllE3gl 4w2GmEKaq+AdYG7j1T5uWVg+sIZ1GCofi/+1ml6U588bqKzUSkjA4Gn+ ZoLToviPSY
t1RYzUc3H72ScM+Kv2o+ZtC2YRSmrnVGqcSTr iysYdlzmU7c=
cn.                     21600   IN      RRSIG   NS 8 1 86400 20231120033617 20231021030649 38388 cn. UdHSOXK4wJ
vtqvxArP9w+Ud36wjruWHGJLWGW8CbWg8fmsl iCcJUNYb3KNupdT86eYV0rpXIBcEWdo8ujID+x4kBugOOVsSzjKGp+zx XgkMqByKXuQ/oLQ/
JRPMiYkB//Ko05ID/AIltaYXqZQ6EJ+ 5Uw=
cn.                     21600   IN      NS      c.dns.cn.
cn.                     21600   IN      NS      d.dns.cn.
cn.                     21600   IN      NS      a.dns.cn.
cn.                     21600   IN      NS      b.dns.cn.
cn.                     21600   IN      NS      e.dns.cn.
cn.                     21600   IN      NS      ns.cernet.net.
cn.                     21600   IN      RRSIG   SOA 8 1 86400 20231125072428 20231026062428 38388 cn. Z2NloyhnZ
iO6jYMUzsHkOm3SV1Y6qdowuYljuJONX5fMGXi JFeIA8qxab5/de3SNmSGsurnKigNsECKYz9gnow/8GZuWUovORTrBrzR 0A1JmYdc4HZOMr6
/TUJ5tlC/YM6oykhHWYSauQW6hd8yrsf DKo=

;; Query time: 291 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Oct 26 15:25:22 CST 2023
;; MSG SIZE  rcvd: 1572

duanhx@MBP-abai ~ %
```




放大倍数=(1420+200)/59=27



# 真实案例

```
16:25:28.581992 IP (tos 0x0, ttl 227, id 17717, offset 0, flags [none], proto UDP (17), length 66)
    54.235.154.83.27284 > 166.111.[redacted].domain: [no cksum] 9579+ [1au] ANY? pkts.asia. ar: . OPT UDPsize=9000 (38)
16:25:28.582021 IP (tos 0x0, ttl 227, id 17718, offset 0, flags [none], proto UDP (17), length 66)
    54.235.154.83.27284 > 166.111.[redacted].domain: [no cksum] 9579+ [1au] ANY? pkts.asia. ar: . OPT UDPsize=9000 (38)
16:25:28.582029 IP (tos 0x0, ttl 227, id 17719, offset 0, flags [none], proto UDP (17), length 66)
    54.235.154.83.27284 > 166.111.[redacted].domain: [no cksum] 9579+ [1au] ANY? pkts.asia. ar: . OPT UDPsize=9000 (38)
16:25:28.582035 IP (tos 0x0, ttl 227, id 17721, offset 0, flags [none], proto UDP (17), length 66)
    54.235.154.83.27284 > 166.111.[redacted].domain: [no cksum] 9579+ [1au] ANY? pkts.asia. ar: . OPT UDPsize=9000 (38)
16:25:28.582418 IP (tos 0x0, ttl 64, id 25028, offset 0, flags [+], proto UDP (17), length 1500)
    166.111.[redacted]domain > 54.235.154.83.27284: 9579 q: ANY? pkts.asia. 243/2/3 pkts.asia. A 1.1.1.43, pkts.asia. A 1.1.1.44, pkts.asia. A 1.1.1.45, pkts.asia. A 1
.1.1.46, pkts.asia. A 1.1.1.47, pkts.asia. A 1.1.1.48, pkts.asia. A 1.1.1.49, pkts.asia. A 1.1.1.50, pkts.asia. A 1.1.1.51,
.53, pkts.asia. A 1.1.1.54, pkts.asia. A 1.1.1.55, pkts.asia. A 1.1.1.56, pkts.asia. A 1.1.1.57, pkts.asia. A 1.1.1.58, pkt
 pkts.asia. A 1.1.1.61, pkts.asia. A 1.1.1.62, pkts.asia. A 1.1.1.63, pkts.asia. A 1.1.1.64, pkts.asia. A 1.1.1.65, pkts.as
s.asia. A 1.1.1.68, pkts.asia. A 1.1.1.69, pkts.asia. A 1.1.1.70, pkts.asia. A 1.1.1.71, pkts.asia. A 1.1.1.72, pkts.asia.
ia. A 1.1.1.75, pkts.asia. A 1.1.1.76, pkts.asia. A 1.1.1.77, pkts.asia. A 1.1.1.78, pkts.asia. A 1.1.1.79, pkts.asia. A 1.
A 1.1.1.82, pkts.asia. A 1.1.1.83, pkts.asia. A 1.1.1.84, pkts.asia. A 1.1.1.85, pkts.asia. A 1.1.1.86, pkts.asia. A 1.1.1.
1.1.89, pkts.asia. A 1.1.1.90, pkts.asia. A 1.1.1.91, pkts.asia. A 1.1.1.92, pkts.asia. A 1.1.1.93, pkts.asia. A 1.1.1.94,
96, pkts.asia. A 1.1.1.97, pkts.asia. A 1.1.1.98, pkts.asia. A 1.1.1.99, pkts.asia. A 1.1.1.100, pkts.asia. A 1.1.1.101, pkts.asia. A 1.1.1.102, pkts.asia. A 1.1.1.1
03, pkts.asia. A 1.1.1.104, pkts.asia. A 1.1.1.105, pkts.asia. A 1.1.1.106, pkts.asia. A 1.1.1.107, pkts.asia. A 1.1.1.108, pkts.asia. A 1.1.1.109, pkts.asia. A 1.1.
1.110, pkts.asia. A 1.1.1.111, pkts.asia. A 1.1.1.112, pkts.asia. A 1.1.1.113, pkts.asia. A 1.1.1.114, pkts.asia. A 1.1.1.115, pkts.asia. A 1.1.1.116, pkts.asia. A 1
.1.1.117, pkts.asia. A 1.1.1.118, pkts.asia. A 1.1.1.119, pkts.asia. A 1.1.1.120, pkts.asia. A 1.1.1.121, pkts.asia. A 1.1.1.122, pkts.asia. A 1.1.1.123, pkts.asia.
A 1.1.1.124, pkts.asia. A 1.1.1.125, pkts.asia. A 1.1.1.126, pkts.asia. A 1.1.1.127, pkts.asia. A 1.1.1.128, pkts.asia. A 1.1.1.129, pkts.asia. A 1.1.1.130, pkts.asi
a. A 1.1.1.131, pkts.asia. A 1.1.1.132, pkts.asia.[|domain]
16:25:28.582445 IP (tos 0x0, ttl 64, id 25029, offset 0, flags [+], proto UDP (17), length 1500)
    166.111.[redacted]domain > 54.235.154.83.27284: 9579 q: ANY? pkts.asia. 243/2/3 pkts.asia. A 1.1.1.44, pkts.asia. A 1.1.1.45, pkts.asia. A 1.1.1.46, pkts.asia. A 1
.1.1.47, pkts.asia. A 1.1.1.48, pkts.asia. A 1.1.1.49, pkts.asia. A 1.1.1.50, pkts.asia. A 1.1.1.51, pkts.asia. A 1.1.1.52, pkts.asia. A 1.1.1.53, pkts.asia. A 1.1.1
.54, pkts.asia. A 1.1.1.55, pkts.asia. A 1.1.1.56, pkts.asia. A 1.1.1.57, pkts.asia. A 1.1.1.58, pkts.asia. A 1.1.1.59, pkts.asia. A 1.1.1.60, pkts.asia. A 1.1.1.61,
 pkts.asia. A 1.1.1.62, pkts.asia. A 1.1.1.63, pkts.asia. A 1.1.1.64, pkts.asia. A 1.1.1.65, pkts.asia. A 1.1.1.66, pkts.asia. A 1.1.1.67, pkts.asia. A 1.1.1.68, pkt
s.asia. A 1.1.1.69, pkts.asia. A 1.1.1.70, pkts.asia. A 1.1.1.71, pkts.asia. A 1.1.1.72, pkts.asia. A 1.1.1.73, pkts.asia. A 1.1.1.74, pkts.asia. A 1.1.1.75, pkts.as
ia. A 1.1.1.76, pkts.asia. A 1.1.1.77, pkts.asia. A 1.1.1.78, pkts.asia. A 1.1.1.79, pkts.asia. A 1.1.1.80, pkts.asia. A 1.1.1.81, pkts.asia. A 1.1.1.82, pkts.asia.
A 1.1.1.83, pkts.asia. A 1.1.1.84, pkts.asia. A 1.1.1.85, pkts.asia. A 1.1.1.86, pkts.asia. A 1.1.1.87, pkts.asia. A 1.1.1.88, pkts.asia. A 1.1.1.89, pkts.asia. A 1.
1.1.90, pkts.asia. A 1.1.1.91, pkts.asia. A 1.1.1.92, pkts.asia. A 1.1.1.93, pkts.asia. A 1.1.1.94, pkts.asia. A 1.1.1.95, pkts.asia. A 1.1.1.96, pkts.asia. A 1.1.1.
97, pkts.asia. A 1.1.1.98, pkts.asia. A 1.1.1.99, pkts.asia. A 1.1.1.100, pkts.asia. A 1.1.1.101, pkts.asia. A 1.1.1.102, pkts.asia. A 1.1.1.103, pkts.asia. A 1.1.1.
104, pkts.asia. A 1.1.1.105, pkts.asia. A 1.1.1.106, pkts.asia. A 1.1.1.107, pkts.asia. A 1.1.1.108, pkts.asia. A 1.1.1.109, pkts.asia. A 1.1.1.110, pkts.asia. A 1.1
.1.111, pkts.asia. A 1.1.1.112, pkts.asia. A 1.1.1.113, pkts.asia. A 1.1.1.114, pkts.asia. A 1.1.1.115, pkts.asia. A 1.1.1.116, pkts.asia. A 1.1.1.117, pkts.asia. A
1.1.1.118, pkts.asia. A 1.1.1.119, pkts.asia. A 1.1.1.120, pkts.asia. A 1.1.1.121, pkts.asia. A 1.1.1.122, pkts.asia. A 1.1.1.123, pkts.asia. A 1.1.1.124, pkts.asia.
 A 1.1.1.125, pkts.asia. A 1.1.1.126, pkts.asia. A 1.1.1.127, pkts.asia. A 1.1.1.128, pkts.asia. A 1.1.1.129, pkts.asia. A 1.1.1.130, pkts.asia. A 1.1.1.131, pkts.as
ia. A 1.1.1.132, pkts.asia. A 1.1.1.133, pkts.asia.[|domain]
16:25:28.582679 IP (tos 0x0, ttl 64, id 25030, offset 0, flags [+], proto UDP (17), length 1500)
    166.111.[redacted]domain > 54.235.154.83.27284: 9579 q: ANY? pkts.asia. 243/2/3 pkts.asia. A 1.1.1.45, pkts.asia. A 1.1.1.46, pkts.asia. A 1.1.1.47, pkts.asia. A 1
.1.1.48, pkts.asia. A 1.1.1.49, pkts.asia. A 1.1.1.50, pkts.asia. A 1.1.1.51, pkts.asia. A 1.1.1.52, pkts.asia. A 1.1.1.53, pkts.asia. A 1.1.1.54, pkts.asia. A 1.1.1
.55, pkts.asia. A 1.1.1.56, pkts.asia. A 1.1.1.57, pkts.asia. A 1.1.1.58, pkts.asia. A 1.1.1.59, pkts.asia. A 1.1.1.60, pkts.asia. A 1.1.1.61, pkts.asia. A 1.1.1.62,
 pkts.asia. A 1.1.1.63, pkts.asia. A 1.1.1.64, pkts.asia. A 1.1.1.65, pkts.asia. A 1.1.1.66, pkts.asia. A 1.1.1.67, pkts.asia. A 1.1.1.68, pkts.asia. A 1.1.1.69, pkt
s.asia. A 1.1.1.70, pkts.asia. A 1.1.1.71, pkts.asia. A 1.1.1.72, pkts.asia. A 1.1.1.73, pkts.asia. A 1.1.1.74, pkts.asia. A 1.1.1.75, pkts.asia. A 1.1.1.76, pkts.as
ia. A 1.1.1.77, pkts.asia. A 1.1.1.78, pkts.asia. A 1.1.1.79, pkts.asia. A 1.1.1.80, pkts.asia. A 1.1.1.81, pkts.asia. A 1.1.1.82, pkts.asia. A 1.1.1.83, pkts.asia.
A 1.1.1.84, pkts.asia. A 1.1.1.85, pkts.asia. A 1.1.1.86, pkts.asia. A 1.1.1.87, pkts.asia. A 1.1.1.88, pkts.asia. A 1.1.1.89, pkts.asia. A 1.1.1.90, pkts.asia. A 1.
1.1.91, pkts.asia. A 1.1.1.92, pkts.asia. A 1.1.1.93, pkts.asia. A 1.1.1.94, pkts.asia. A 1.1.1.95, pkts.asia. A 1.1.1.96, pkts.asia. A 1.1.1.97, pkts.asia. A 1.1.1.
98, pkts.asia. A 1.1.1.99, pkts.asia. A 1.1.1.100, pkts.asia. A 1.1.1.101, pkts.asia. A 1.1.1.102, pkts.asia. A 1.1.1.103, pkts.asia. A 1.1.1.104, pkts.asia. A 1.1.1
.105, pkts.asia. A 1.1.1.106, pkts.asia. A 1.1.1.107, pkts.asia. A 1.1.1.108, pkts.asia. A 1.1.1.109, pkts.asia. A 1.1.1.110, pkts.asia. A 1.1.1.111, pkts.asia.
1.1.112, pkts.asia. A 1.1.1.113, pkts.asia. A 1.1.1.114, pkts.asia. A 1.1.1.115, pkts.asia. A 1.1.1.116, pkts.asia. A 1.1.1.117, pkts.asia. A 1.1.1.118, pkts.asi
 1.1.1.119, pkts.asia. A 1.1.1.120, pkts.asia. A 1.1.1.121, pkts.asia. A 1.1.1.122, pkts.asia. A 1.1.1.123, pkts.asia. A 1.1.1.124, pkts.asia. A 1.1.1.125, pkts.asia
. A 1.1.1.126, pkts.asia. A 1.1.1.127, pkts.asia. A 1.1.1.128, pkts.asia. A 1.1.1.129, pkts.asia. A 1.1.1.130, pkts.asia. A 1.1.1.131, pkts.asia. A 1.1.1.132, pkts.a
sia. A 1.1.1.133, pkts.asia. A 1.1.1.134, pkts.asia.[|domain]
```

$$\frac{\textit{response size}}{\textit{query size}}$$

包放大倍数：
～40（1500/38）

# DNSSEC, Any


[redacted].gov. 6521 IN SOA auth00.ns.uu.net. hostmaster.uu.net. 994278 1800 600 1728000 21600
[redacted].gov. 6521 IN RRSIG NSEC3PARAM 7 2 21600 20160311030329 20160304020329 27102 [redacted].gov. JwsCXTa2gH68/7q+tenYkxtPm6vc8SPSpAixY/ldZtNmxWIhS0Qd/lSs Bt9JIi2TUS5vzo2k0jxNePYUBjvP4oiw4MQrRMpzxG61DnNSd29aXyK3 wDpFvGvF2iqf3zgP7D2CCmUTjIHEYcXEoLZxCh07JoFpd9gCGfV1UuUG 7+SKfdkNK7PRwMAEHR2duC9OBrnld1ObwScRmCADBldCcE8qeb8A/cc/ CYWGNZwSVBFeNx4mgjvXiKV2zzP9uDiSNvm0OId1+a3+DBi0lpirkGwe VY9kEVshm84y8JlDeyMSofiylKcUJ6l0VuNqRjuuXInY74ftSsHMG1h1 NekTxA==
[redacted].gov. 6521 IN RRSIG DNSKEY 7 2 21600 20160311030329 20160304020329 4696 [redacted].gov. VDtT04MZP1IKN69OkZpuN3JKxYfKdEFOzkCI0v4Cfc4OkXVZUkR5VE8n OCcpEIdgTYX6grYnjrJfPL7ypRlzpu6Yz37aZasdYzT1f5WH1A6MZj9g z2KLWJb/ hRZxpXtAHzhc1vIBuRTBlaOrbqvuVkYupHFQOFsmcSC8MyjR qYgEb/ SeqgWGh33nTGDectee97qNkP5bC1AK+f3m1FdSTUdiCafKxDHD xfLxC6HNha9p2EXrZGWvNOUbWkKykEvUNCkQ0jvDjbB54q0DMzcrZqXC pXA2l0nHDb4HB8g2OZsUIGtDttaXgmIc/OR4bqh3RIU+tARK4mDOfWl5 80yRVA==
[redacted].gov. 6521 IN RRSIG DNSKEY 7 2 21600 20160311030329 20160304020329 27102 [redacted].gov. okImbgNqbvYu+N4xo4CPQ1tFjKwuqpCbtcXg4jQVaFnMpaJORrp6dMfi ToGg8hxt47ky3nbOQprfsSluJm0MygSUnVY9FpyEnW7H56gUGKk1fsNp Ar1CBxWgz342vjPxyWxcPbOPowlONXy9CRKA32k23T9OntsVDwCvuSpO EqFPHJb/ sNosRCyoXLxIH29Qwy3gfe65X/CA9TWXekbzhNs5Gkbchuvc 6EfWLAbzZ88TUcsH2otULBFxRCD/ 9Njo3/7a2yma4daVtWBVr7Oapsk9 Lq3ZeKS97Ocj4olAZ8ZAjMtp6wO26EjETFGhJ6qkaJFUJDknX2iyQ4Or Cgd5zw==
[redacted].gov. 6521 IN RRSIG SOA 7 2 21600 20160311030329 20160304020329 27102 [redacted].gov. CKQO/iNpHjwgmDRI4FBq53HoqivZeqSLRwXCfo27uwBQ4aQS+4AnZK+s 8IyJjC1e5rrcOGCFIJ4h6sYz+MGhtgVaI0LPddoEk7/sGuKCHUopEnOK wx6n/ 6/3+C5QKZ20enbaVBRLwFsmvmvCg0d5gqjoGt8zSvMfjB+pWh2F almGzArBLcfDH1R3osDNAQnklt0mnwkXjIO0eqhUGz+ddrh1TT9rHIBa sP0czl3woESGGxTumL1NrhPkyEQPN7hp3uev/ug332ZkHDbla1FPJg+U HpLM7MUImtS2eIH844rm2VsmRGOeLNgtCZjjVho+P+EK2o+oOHfZCgUl ZFuqHQ==
[redacted].gov. 6521 IN RRSIG AAAA 7 2 21600 20160311030329 20160304020329 27102 [redacted].gov. WXAtUkhSVrEsM/8QEZg74gbHcRkbBPiJieP7bGxQbQ/Q5JCXIWO1k519 RrzrdyYBqyUk8YCTLaaB5K3DVMIkWBTFlK6KaRNE84z/2/DG6kNeM+au nqIN7AZunuVGsbH1mkm/ QYFVr/Cza8JxKdyhaVCtIMAr2KzD0Quy47FQ 5GKSC +GL1EhtZPrMo6YBK7oJ1PXCZzz40Zbq4pT92DYxIRxwzZTJYktd IC4ISVYpvD5fzCi +cV5IuAV2LRigP34x70qgLOYh+N/7qtScTbrDBCGb rMXzv3HyKgk9frBkKTWlyXPEURCVSBpzXQPPRhiNUikqXjlmd7bV8vfM GyCZZQ==
[redacted].gov. 6521 IN RRSIG A 7 2 21600 20160311030329 20160304020329 27102 [redacted].gov. W0oir8d7DVaP5U4VrjjKs9gUC3FohJUSVs1ZWpZ7BhUxEahu2Q2Eesq5 fVVOF1lsI/G/r/w +bNfNH4HPMYW02IqtDtzDUe9rsylZhC96tHNb9VOR x1MxQTAjWwIsnbUReTqa9FBjWV4VsIS7mZkbdheuXP0BRUNU/G9/Zmux NebPTxcbGOxGqLayYYbjOoNEJFhU2e7JsjqPg7IYyVmeVG8lPbn4713w B5OsO7AqV0jaNBfAyXAVI0iuSUU+iJo0/ruNfeseHCP/BZ3SfNjgN/d6 0zl4qQFoTXuK3aK82vMEJtLGQ2R9xkdX5E5VD3POQMvrlzmlgvWWCMrY sJxf2w==
[redacted].gov. 6521 IN RRSIG TXT 7 2 21600 20160311030329 20160304020329 27102 [redacted].gov. ULVsCq0b4svmD7prSjHLt86JscZN5UETCYNNeCJnKKYF4MG96sk8jgUA M3ZEXwr8G0gI/ fIYWVYNzdyexSMcw1VfWcrcahGo0o8rCAckAfazrH+u JKfQ5wVbHLukKkh3KenPDd5QO5X9+n +xu7dfOERVEJo8CwEr7MAgrsOk i4ROYqXdvdnbQsqiqr4vf6lCugE0aqVStqww +K2KBg87uM0VZw2nqoVR k28nopjjkFV+4BIxdTl3+adcRU9ObqupnhzZxbBholQatggmo/Ywz7ss OvSAl9n8ec3FVymH1s7hS3fpSZQnnV/TNS3MAAMwEYtyTbHI29g3bBZQ 1JTDBg==
[redacted].gov. 6521 IN RRSIG MX 7 2 21600 20160311030329 20160304020329 27102 [redacted].gov. eapoSW9qROOuzCROJC3hIL40qkX0z5cSIpneGa8kjwHUf4VqMSo0Ryiy CjL1mVUttiwNZV4Z0r2rBKLafPl20pC5rMoWZpIMjc2SNlWGeH8ZzZY9 +f4gjL+d3UF5d+KmODLD/ r0nQ5Ti/qnYPRD061McUZz+R6gj1WNHUcja bYCa1VaiS1ZfEL9+3xQTqOuF86nv3m9VIDgfjSZjw5F5lkFsi95PTseO kz6/ eAz5ScODgUa5NKqBdA6cNmDK89RxONYy/Pd1TM6j24Uf7SWMFF0l 1ssnXZwOgXOtGTtZNjlLOfCTTGvcaz5s2qeT8xZzU09Rsad5rCm9Q60D yAVXuq==
[redacted].gov. 6521 IN RRSIG NS 7 2 21600 20160311030329 20160304020329 27102 [redacted].gov. PzR6EkmB6vq+dD9GK71XKMGW3bHXHXbPdKOaQcawY3fzfAytvyaFTUGq lKRALQ6elS8w4QOzPtimvwITtji1ClgwTgkxO43eY2duS2x2AkSeHY8+ obBjnVYAjxgERpbp12TU7Tel T0E/3RK62ru/2wdrVlSxGGyawHYxaXKM N2MTEThB+X7B0hR1km// jhjrhYHrkqU4LI2TGcqzVpIXx1me5oPOIj9i Acn2hDWiZZSfP8TSYwuha+sHkLtfP/ U02bGolxd7wN67uEz2c9v93X+j pE4F/ ZGOEtzM2CV2oWvO2blsw8oXo56zcrAIMNOxi0YoaIsF3QVYQtDF XZMvoQ==
[redacted].gov. 6521 IN NSEC3PARAM 1 0 12 AABBCCDD
[redacted].gov. 6521 IN DNSKEY 256 3 7 AwEAAYj4CFvFWz05HXMTladmoNqrrClt0RasgJUU9Eal WW8FkatpEu8e jSnq3UeV3lqAT/nlYOxb/ lCH2bW+a+lCJ4ircz7VajdFedFRXuZxOmDr p8ca4/zhQLBpwuAITiJRzLPgEQuPKTYEi/bTpvTx2pU +wza0seBp7ucC u+JYuQNw0lHSUCSqZovru+6npbR25WXwqJ3aY89fUfHLZ1so4znc6lH2 xchAbhyabbyqkH23+vr2tE27AJLg/BffDLS8DQ/QbDiBAMcsch380joF wzB9K4IbJGGk6fagwUON2KqRwDiZHeWUBAsjthTswpPGdf2+DvtvBkyL +8m4eOd2hjk=
[redacted].gov. 6521 IN DNSKEY 257 3 7 AwEAAX5Tor9V7TnhfUMAL67reT+IFYd+4ciQv/ UnvZbNgj7DgDuJPpcl Owh6ypAldCYgTXkF2Qt+an9WVp+Khsp2wRCCOhvGIUR9sOGdzxumDUCT Uru2dxHAqIn1QYSjuT8huMDDyBJmnoA4AY1Te86mcE1Jwpo+S9KoB23Z JgnMedU +6i8Qm9cdGLNM7nqEXhgKgmKc/387UFdh25jltsg0d2gOK//q k2HfldDqv8XlrlacfMsSXniVwK7E6mtqcfbF518M2bl6UFJWXuxp+cU8 0WdmGiQfxmLvm62a2aVs9IzR6qGg0Ce5bxbx68v6gYTgIOUBm8ERytZ3 T2jzc0QOKQc=
[redacted].gov. 6521 IN DNSKEY 256 3 7 AwEAAd5i4It5aUL97Y2LWx7N/1/ orV3dW0CZS255wyWU2WcN6ecAKFCP 4IJhWTA61XM9qJNzQVvGPeu0krbok3M9GrgnmVbW2f/ oGMmte7pAHDrb +ccmpOnJyas6qsbJNO2ldTHtiEXqHsKJ//TEfTyAVtadDj7PUQBbSCdP wdvoC5EmMnJzzuBtctNG2ZkrQZ6Co9t8RS3ueQK50uvXnldnhyv4Mbrl CauD7TXlChYjTe05BCRYzJM3fHDokHhExASqZupzsMF+6mvUylJXtUJr BqDHvn6jrry8HIW9t8y/ eN7UOMUJJP4HuVnlpeEQHJ6q0Kdlr3E9nSNI cHCM9fVZuVc=
[redacted].gov. 6521 IN DNSKEY 257 3 7 AwEAAZJY5dIAm8QsM2sBBsOoYkeMhklsUHBqMOAlxQ8VBhoVNoDN0vVz OpLAGVTEThzvOllLX2WxCpkU8AKioO4l188RjBf5wjs/Aj2i1uI8QIyh aMxZS/ ifWgR4bBA4d4NgGDpHZElr0Cn2OlDJwhGENOr9kxhgDXT97UVn I2F7JptQZgeAIlGowVPMUpSz4v6l0ueyOgYWNYN03+IitYOWHMDBm4t3 oYhrCKnqPuauGloulWS9y5eaYNR82j/WnCzAK/gb5XTcHi02JB98PiAX UO7+CNji9ZRt/ yFDqpogoKh3oqvEC+lPNAP9CZ/DuUp+RDL41mm5vKvp F9geIq5XGFE=
[redacted].gov. 6521 IN AAAA 2600:803:240::2
[redacted].gov. 6521 IN A 63.74.109.2
[redacted].gov. 6521 IN TXT "v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.[redacted].gov -all"
[redacted].gov. 6521 IN MX 5 stagg.[redacted].gov.
[redacted].gov. 6521 IN MX 5 hormel.[redacted].gov.
[redacted].gov. 6521 IN NS auth00.ns.uu.net.
[redacted].gov. 6521 IN NS auth61.ns.uu.net.

[4106 bytes]

cloudflare.com. 3789 IN HINFO "Please stop asking for ANY" "See draft-ietf-dnsop-refuse-any"
cloudflare.com. 3789 IN RRSIG HINFO 13 2 3789 20160305195721 20160303175721 35273 cloudflare.com. mvNGF8SJemg6UpifhakygI6YL7sC0VR9vrRfdI8mMamEZW6wmEsB05k6 oo6bCzzYHLlctICatkxgItAc5uKFLQ==

[231 bytes]

```
duanhx@HaixindeiMac-Pro ~ % dig @8.8.8.8 +dnssec any x.com

; <<>> DiG 9.10.6 <<>> @8.8.8.8 +dnssec any x.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28990
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;x.com.                         IN      ANY

;; ANSWER SECTION:
x.com.                  3600    IN      HINFO   "RFC8482" ""

;; Query time: 94 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Oct 17 18:05:10 CST 2024
;; MSG SIZE  rcvd: 55
```

Internet Engineering Task Force (IETF)
Request for Comments: 8482
Updates: 1034, 1035
Category: Standards Track
ISSN: 2070-1721

J. Abley
Afilias
O. Gudmundsson
M. Majkowski
Cloudflare Inc.
E. Hunt
ISC

January 2019

# Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY

## Abstract

The Domain Name System (DNS) specifies a query type (QTYPE) "ANY". The operator of an authoritative DNS server might choose not to respond to such queries for reasons of local policy, motivated by security, performance, or other reasons.

The DNS specification does not include specific guidance for the behavior of DNS servers or clients in this situation. This document aims to provide such guidance.

This document updates RFCs 1034 and 1035.

# DNS反射放大攻击的防范

- Close your open Resolvers
- Source address Validation
- Rate Limit of DNS query
- Disable  ANY  query
- Load Balance of DNS Authority server
- Cloud Service: Akamai, CloudFlare, AliCloud…

# 负载均衡实例: mit.edu

```
duanhx@MBP-abai ~ % dig www.mit.edu

; <<>> DiG 9.10.6 <<>> www.mit.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30769
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.mit.edu.                   IN      A

;; ANSWER SECTION:
www.mit.edu.            1800    IN      CNAME   www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net. 60     IN      CNAME   e9566.dscb.akamaiedge.net.
e9566.dscb.akamaiedge.net. 20   IN      A       184.26.247.103

;; Query time: 667 msec
;; SERVER: 10.6.6.1#53(10.6.6.1)
;; WHEN: Thu Oct 26 15:45:51 CST 2023
;; MSG SIZE  rcvd: 132

duanhx@MBP-abai ~ % dig ns edgekey.net.

; <<>> DiG 9.10.6 <<>> ns edgekey.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14757
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 21

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;edgekey.net.                   IN      NS

;; ANSWER SECTION:
edgekey.net.            115062  IN      NS      a9-65.akam.net.
```

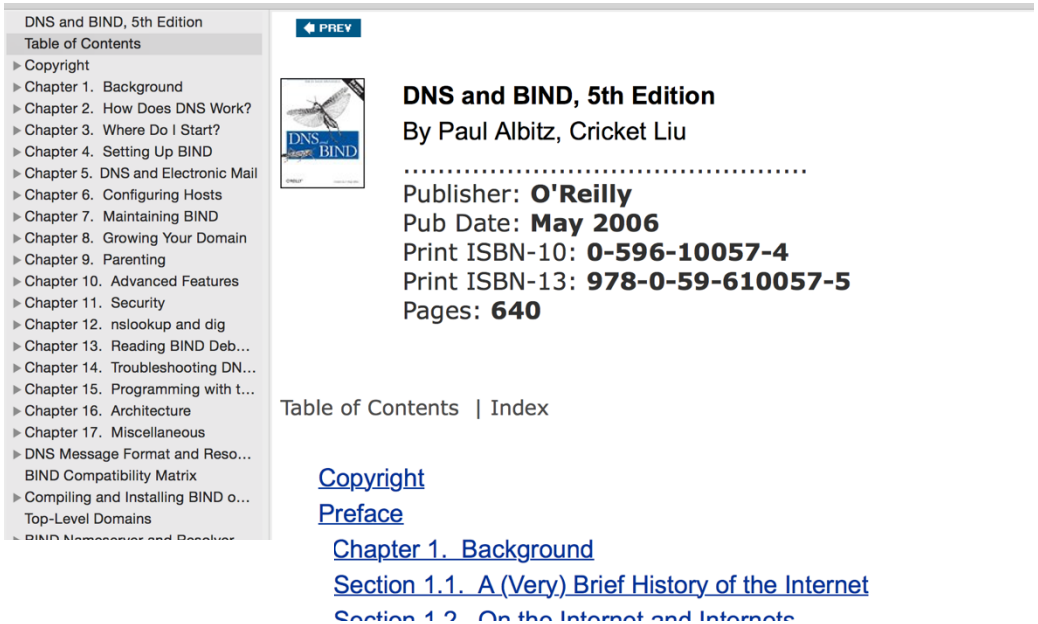
```
duanhx@MBP-abai ~ % dig ns edgekey.net.

; <<>> DiG 9.10.6 <<>> ns edgekey.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14757
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 21

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;edgekey.net.                   IN      NS

;; ANSWER SECTION:
edgekey.net.            115062  IN      NS      a9-65.akam.net.
edgekey.net.            115062  IN      NS      a13-65.akam.net.
edgekey.net.            115062  IN      NS      a16-65.akam.net.
edgekey.net.            115062  IN      NS      a11-65.akam.net.
edgekey.net.            115062  IN      NS      ns1-2.akam.net.
edgekey.net.            115062  IN      NS      adns1.akam.net.
edgekey.net.            115062  IN      NS      a28-65.akam.net.
edgekey.net.            115062  IN      NS      a3-65.akam.net.
edgekey.net.            115062  IN      NS      usw6.akam.net.
edgekey.net.            115062  IN      NS      a6-65.akam.net.
edgekey.net.            115062  IN      NS      a12-65.akam.net.
edgekey.net.            115062  IN      NS      a18-65.akam.net.
edgekey.net.            115062  IN      NS      a5-65.akam.net.

;; ADDITIONAL SECTION:
a3-65.akam.net.         88941   IN      A       96.7.49.65
a5-65.akam.net.         62791   IN      A       95.100.168.65
a6-65.akam.net.         42482   IN      A       23.211.133.65
a9-65.akam.net.         13544   IN      A       184.85.248.65
a11-65.akam.net.        75901   IN      A       84.53.139.65
a12-65.akam.net.        115062  IN      A       184.26.160.65
a13-65.akam.net.        88631   IN      A       2.22.230.65
a16-65.akam.net.        115062  IN      A       23.211.132.65
a18-65.akam.net.        115062  IN      A       95.101.36.65
a28-65.akam.net.        115062  IN      A       95.100.173.65
a3-65.akam.net.         88941   IN      AAAA    2600:1408:1c::41
a5-65.akam.net.         7382    IN      AAAA    2600:1480:b000::41
```

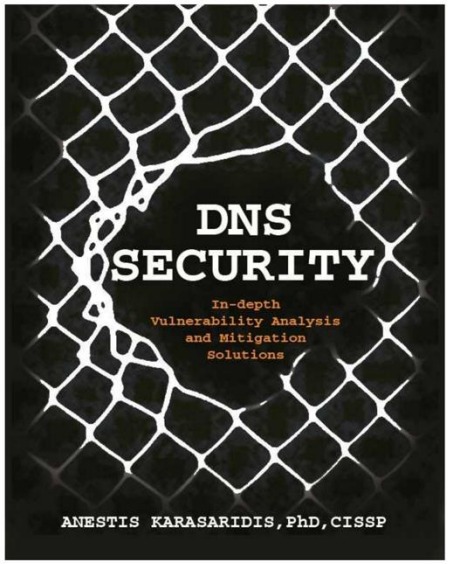
# Summary

- DNS作为最重要的互联网基础服务
- 了解DNS的攻击原理
- 根域名服务器的部署
- 针对DNS的攻击，如Cache Poisoning
- 利用DNS 构造的攻击，如DDOS

# Reference

**DNS and BIND, 5th Edition**
By Paul Albitz, Cricket Liu
.....
Publisher: **O'Reilly**
Pub Date: **May 2006**
Print ISBN-10: **0-596-10057-4**
Print ISBN-13: **978-0-59-610057-5**
Pages: **640**




**DNS Security**
by Anestis Karasaridis, PhD,CISSP

https://www.amazon.com/gp/product/B007ZW50WE/ref=kinw_myk_ro_title

# Lab2：DNS缓存污染攻击