SAC 056

SSAC 关于通过域名系统内容阻止所产生的影响的咨询报告

ICANN 安全与稳定
咨询委员会
咨询报告
(SSAC)

2012 年 10 月 9 日

序言

本文是安全与稳定咨询委员会(SSAC) 的一份报告。SSAC 负责针对互联网名称和地址分配系统的安全性和完整性向 ICANN 机构群体和理事会提供有关问题的建议。这包括运作问题（例如与正确、可靠地运行根域名系统有关的问题）、管理问题（例如与地址分配和互联网号码分配有关的问题）以及注册问题（例如与注册管理机构和注册服务商提供的服务有关的问题）。SSAC 一直从事互联网名称和地址分配服务的威胁评估和风险分析工作，评估哪里存在严重的稳定性和安全性威胁，并据此向 ICANN 机构群体提供建议。SSAC 不享有监管、强制执行或裁定的职权。这些职能属于其他机构，对于本报告中列出的建议，应根据建议自身的价值予以客观的评估。

本报告的末尾列出了报告的编著者、关于委员会成员个人简介和利益声明的参考文档以及委员会成员对报告中各项调查结论或建议的反对意见。

目录

1. 执行摘要

通过“域名系统 (DNS) 内容阻止”来限制对互联网资源的访问，这一做法已受到众多互联网监管机构的关注。世界各地的一些政府通过章程、条约、法院指令、执法行动或以其他行动或协议的形式，已开始实施 DNS 阻止或积极考虑采取该项措施。然而，由于互联网的架构问题，通过域名系统来阻止访问很容易被最终用户所规避，因而长期来看，这可能会收效甚微，短期来说，也会伴随产生许多不可预料的后果。此外，DNS 阻止可能与域名系统安全扩展 (DNSSEC) 相冲突，而且会导致互联网的割据化 — 互联网域名空间被划分为一个个的“小王国”。

本文档仅限于探讨与 DNS 阻止有关的技术影响，包括：

- 通过以下途径实施的域名阻止：
  - 注册管理机构或注册服务商；
  - 权威服务器；
  - 通过递归解析器中的重定向、“域名不存在”响应代码、“查询被拒绝”响应代码、其他响应代码或“查询无响应”。
- 递归解析器内实施的 DNS 阻止及与 DNSSEC 的冲突；
- 使最终用户趋向于端到端加密；
- 过度阻止；
- 拼字错误；
- 避开实施阻止的国家来路由 DNS 流量；
- 用户切换解析器所产生的影响；及
- 用户切换解析器对内容分发网络 (CDN) 本地化的干扰。

此外，还有一些非技术类问题（如对言论自由的限制），这些问题不属于本文档的讨论范围。互联网团体、政府及其他机构需理解并认真考虑与 DNS 阻止有关的所有问题 — 包括技术类和非技术类问题。

2. 简介

本文档在“SAC050: DNS 阻止：利与弊 – 安全与稳定咨询委员会的咨询报告”的基础上编写，感兴趣的读者可以参考。[1]

在 2011 年和 2012 年，多个政府拟议或制订了与 DNS 阻止、DNS 过滤和/或域名捕获相关的正式指导准则、法规、法庭指令或执法行动。[2]在某些情况下，这些行为旨在制订新的法律来控制互联网的使用，还有一些情况是，执法机关以 DNS 阻止或域名捕捉为手段来阻止访问特定的互联网站点或地址。[3、4、5、6]

本文将研究目前已实施或提出的各种 DNS 阻止方式在技术层面上的影响。本文旨在向互联网群体、政策制订者、政府工作人员和其他人群提供信息，让他们了解用来控制互联网资源访问的 DNS 阻止有何高端层面的技术性影响。[7]

3. DNS 阻止：利与弊

SAC050 的主要结论为：

> “域名或基于 Internet 协议 (IP) 地址的过滤（或阻止访问会让计算机感染病毒的网站内容，或防止对雇主资源构成不当使用的行为）对于某些组织机构而言，可能就相当于以往禁止组织内部员工拨打私人电话而产生巨额话费那样。
> …

[1]请参见“SAC050: DNS 阻止：利与弊 – 安全与稳定咨询委员会关于使用域名系统阻止顶级域名的咨询报告”，ICANN（互联网名称与数字地址分配机构）安全与稳定咨询委员会，2011 年 6 月 14 日，http://www.icann.org/en/groups/ssac/documents/sac-050-en.pdf。

[2]请参见 H.R. 3261（反网络盗版法案），美国众议院，第 112 届国会，2011 年 12 月 16 日版本，以及爱沙尼亚有关阻止访问非法赌博网站的法规，https://www.riigiteataja.ee/akt/125042012010。

[3]请参见 OpenNet 动议，http://opennet.net/youtube-censored-a-recent-history。

[4]请参见 http://arstechnica.com/tech-policy/2011/01/amidst-chaos-and-riots-egypt-turns-off-the-internet/。

[5]请参见 http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm.

[6]请参见 http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html。

[7]要了解 DNS 的相关信息，请参见 http://queue.acm.org/detail.cfm?id=1242499

> 无论采用何种机制，实施阻止的组织都应采用以下原则：
>
> 1. 组织针对网络及其用户实施管理控制策略（它是策略域的管理员）。
> 2. 组识认为策略的实施对其有利并符合用户的需求。
> 3. 组织使用对其网络运营和用户具有最低干扰性的技术来实施该策略，除非法规指定了特定的技术。
> 4. 组织共同努力确保实施该策略不会对策略域之外的网络或用户造成损害。
>
> 如果这些原则没有得到落实，使用 DNS 阻止会导致间接损害或意外后果，且很少能或无法为受影响的各方提供补救措施。”

将 SAC050 的结论展开来看，适当的考量及互联网整体稳定性要求我们在实施任何 DNS 阻止策略或行动之前，应向受影响的各方（包括最终用户、服务提供商和应用程序设计者）完整披露这些策略和行动。如果没有披露即实施 DNS 阻止，将会导致不必要的故障排除工作，以及网络操作员或最终用户主动或无意间采用的绕开阻止措施的行为。此类信息披露应包括实施阻止的原始动机、想要达成的效果以及预期的负面作用。如果没有这样的透明度，DNS 阻止可能会被误认为网络中断或者恶意攻击，导致最终用户、网络管理员和服务提供商等去尝试缓解本不存在的问题。

这很可能导致对网络的错误诊断，而且用户不可避免地要去寻找解决方案，进而导致连带损失或意外后果。联合国促进和保护意见和言论自由权问题特别报告员在《联合国人权事务高级专员办事处报告》中也呼吁开展独立的公众审议，报告中提到：

> “31.[…]第三，即使有正当的实施理由，阻止措施也是一种为达成所需目的而采用的不妥当或不合适的方式，因为这类方式通常针对性不足，造成一些原本不是非法内容的资源也无法访问。最后一点，内容的阻止通常欠缺司法或独立机构的介入或审查。”[8]

该文章其余部分还探讨了 DNS 阻止手段的类型和影响。

[8] FrankLaRue，“联合国促进和保护意见和言论自由权问题特别报告员的报告” A.HRC.17.27.，http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf。

4. 互联网架构中的内容阻止

互联网架构的一个基本原则是“端到端”概念，它将网络核心（中间）的智能需求降到最低，转而采用边缘智能（各个主机）的模式。此架构使得一种创新的交互方式得以实现并产生广泛和深远的影响，例如，网络一端的开发人员可以在主机上部署新应用，而另一端的最终用户可以安装相应客户端，两者之间进行交互，而无需任何特别权限或者在网络的任何部分进行特殊控制。

通过域名系统实施内容阻止某些时候发生于互联网的“核心”，某些时候则发生于互联网的“边缘”。访问提供商、其流量来源及流量接收方之间的连接称为“边缘”。运营商内部或运营商之间的连接则称为“核心”。在网络连接的某一端使用网络浏览器黑名单和 IP 流量过滤，这是在边缘实施阻止的例子。如果在网络核心实施边缘模式的阻止，受影响的最终用户可能会通过变更 DNS 服务提供商或使用 VPN、代理或插件的方法来避开阻止措施。要使边缘模式的 DNS 阻止有效，需满足以下条件：相关最终用户同与其交换数据包的任何网络之间的所有路径都采用了基于策略的过滤手段。国家级和企业级的防火墙都属于这类拓扑结构。

这种架构的一个副作用是，在除网络边缘以外的其他任何位置对流量进行阻止 — 无论是基于域名（如 example.com）还是基于 IP 地址（如 192.0.2.117），用户都有可能借助虚拟专用网络 (VPN) 等手段加以突破。[9]一般用户也很容易获得 VPN 和类似方法，而且使用起来并不复杂。即便对互联网的访问网络实施完全的管理和运营控制（例如在互联网服务提供商内部或者某些互联网中继点），[10]最终用户仍有可能访问受阻止的内容。[11]

那些相对更为有效的过滤方法有一个共同特征，即最终用户和网络运营商对于过滤哪些内容以及采用何种方法来过滤内容等问题明确或默认达成一致。在这种情况下，最终用户会将 DNS 阻止视为一种有价值的服务。

[9]请参见 http://www.prlog.org/11725655-how-to-bypass-blocked-sites-with-vpn-account.html 或 http://vpn-account.com/bypassblockedsites.html。

[10]请参见 http://en.wikipedia.org/wiki/Internet_exchange_point。

[11]请参见 http://www.foreignpolicy.com/articles/2011/01/26/can_governments_really_block_twitter。

5. 所实施或提议的 DNS 阻止手段的类型

最近几年提出或实施了多种阻止 DNS 的方法。相对而言，某些方法会带来更多的技术隐忧，下面我们仅列举数例：

1. **通过注册管理机构或注册服务商来捕获域名：**这一方法通过 DNS 注册管理机构或担当这些机构代理的注册服务商将 DNS 数据从来源处清除。注册管理机构是负责创建 DNS 数据（包括指定要阻止的域名）的权威数据库的主管机构。例如，政府可以下达域名“除名”指令至需要依法执行这一指令的注册管理机构或注册服务商。注册管理机构或注册服务商根据此类“除名”要求所采取的反应依指令的具体内容而定。可能的行为包括：将域名从特定区域（即所谓规定该域名注册数据维持时间的“域名保留”记录）移除，从而避免最终用户解析与特定站点关联的域名；或者将域名映射至另一个名称服务器，将用户重定向至显示特定信息的页面 （例如告知用户该域名已被除名）。在“域名保留”情况下，一旦超过域 DNS 记录的“生存时间”(TTL) 设置（通常为数小时或数天），该域将变成在全局范围内不可解析。这意味着用户在输入该域名时，系统将返回“域名不存在”的消息。如果捕获到正确的域名，单就“域名保留”方法而言，不会有任何直接的负面技术性影响。间接的负面技术性影响包括，如果有其他域依赖于被移除的域名上的名称服务、电子邮件服务或 web 服务，则远程服务将会失败。就“域名保留”或名称服务器变更的方法而言，注册服务商或注册管理机构还必须更新或移除所涉及域的任何 DNSSEC 数据。如果没有更新或移除这些数据，将会导致与 DNSSEC 兼容的应用程序在响应 DNS 查询时检测到无效数据，从而无法进行任何通信，甚至会导致向用户解释该域为何不可访问。
2. **权威服务器中实施的域名阻止：**此类型的阻止由受影响域名的权威域名服务器的运营商实施，它能绕过注册管理机构，还有可能绕过注册服务商，直接作用于域名在互联网上生效所依赖的机制。一旦注册者取得并正确配置其域名，注册机构将生成 DNS 数据并将其发布至一组“权威服务器”。很多情况下，这些权威服务器由注册服务代理商运营，但并非所有情况都必须如此，且一个域的权威服务器也无需由同一个机构运营。无论权威服务器的运营主体是谁，这些服务器的作用都是发布网站，因此可对其实施 DNS 阻止措施。例如，政府可向运营该域名的权威服务器的服务商下达域名“除名”指令。运营服务商随即移除或修改该域名的权威 DNS 记录副本。如果这一除名指令下达至该域的权威服务器的所有运营商并得以执行，该域将立即在全局范围内无法访问，在超过域 DNS 记录的 TTL 设定时间后，将最终无法解析。除了要求不同的机构实施阻止之外，此方法与基于注册管理机构或注册服务商而进行的阻止的不同之处在于，如果 DNSSEC 在使用的话，它可能会造成麻烦，因为在变更注册管理机构的域内容时，权威服务器的运营商可能无法保留注册服务商的 DNSSEC 签名。

3. **递归解析器中实施的域名阻止：**递归解析器常用来结合一些商用或开源工具来实施 DNS 阻止，它可让解析器运营商轻松实施阻止。[12] 然而，由于 DNS 架构的原因，在递归解析器中实施的阻止最容易被突破。递归解析器通常由最终用户的 ISP 所运营，在收到最终用户的请求时从权威服务器获取 DNS 数据。最终用户如果希望连接至网站或其他服务，递归解析器会将该网站或服务的域名转化为 IP 地址。通过递归服务器实施的 DNS 阻止，其目的是过滤、编辑或阻止这一转换功能，这可通过多种方法实现：

    a. **通过重定向：**在这种递归服务器阻止方法中，来自权威服务器的响应被修改替代为 DNS 阻止策略所指定的值。例如，递归服务器不会返回要阻止访问的 Web 服务器的 IP 地址，而是返回一个修正服务器的 IP 地址，并显示一则消息，提示用户已阻止对该站点的访问。[13]

        这种阻止方式需要修正服务器能够支持原始目标服务器支持的任何协议或服务，显示重定向提示消息才有技术可行性。也就是说，如果所阻止的目标服务器利用文件传输协议 (FTP) 来提供内容，则用户重定向到的服务器也必须使用 FTP 协议才能显示提示消息。[14] 由于某些协议采用特别的运行方式，此类重定向不一定在任何时候都可行。[15]不过，对于万维网的核心协议 — 超文本传输协议（HTTP）等一些常见协议，此类重定向是可以实现的。

    b. **通过“域名不存在”(NXDOMAIN) 响应代码：**与重定向类似，此类阻止方式修改权威服务器的响应；但它会提示所请求的域不存在，而不是返回另一服务器的 IP 地址。

[12]请参见 http://blog.operationreality.org/2011/10/05/belgian-isps-to-block-pirate-bay-domain-names/ 和 http://news.cnet.com/8301-13578_3-57472718-38/pirate-bay-blocks-did-little-to-curb-file-sharing/。

[13]请参见 http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf。

[14]请参见以下链接中有关“文件传输协议”的说明：http://en.wikipedia.org/wiki/File_Transfer_Protocol。

[15]请参见以下链接中的“COM 和 NET 域中的重定向（2004 年 7 月 9 日）”，ICANN安全与稳定咨询委员会：http://www.icann.org/en/groups/ssac/report-redirection-com-net-09jul04-en.pdf。

c. **通过“查询被拒绝”响应代码：**DNS 协议的 REFUSED（拒绝）响应代码用来指示域由于管理方面的原因而无法解析。这种 DNS 阻止是通过将权威服务器响应修改为针对被阻止的域的 REFUSED 响应来实现的。

   对此 DNS 协议规范的一个有效而合理的全面理解是，REFUSED 响应代码表示不应查询相应名称服务器，否则可能会导致操作系统从其名称服务器列表中将该递归解释器移除。这是因为 REFUSED 响应会被解释为客户端和客户端所请求的所有域名的访问控制问题，而非解释为拒绝应答某些特定域名。如果有足够数量的最终用户查询，此类阻止可导致最终用户所使用的所有名称服务器均被移除，造成最终用户的计算机无法（或不愿意）查询任何名称。因此，解析器针对被阻止域而返回 REFUSED 代码，很可能会造成无法接受的连带损失。

d. **通过其他响应代码：**DNS 协议还提供了一些可用来指示某个域无法解析的响应代码 — 这些代码通常会指示发生了某些类型的错误。这类响应代码包括“服务器故障”(SERVFAIL)、“未实施”(NOTIMPL) 和“格式错误”(FORMERR) 等。

   与 REFUSED 一样，通过这些响应代码进行阻止可能会导致操作系统将递归解析器认定为出错，并将其从操作系统所查询的递归名称服务器列表中移除。因此，所有这些响应方式均不适合用于实现 DNS 阻止。

e. **通过“查询未响应”：**最后要提到的是，递归解析器可以配置为忽略对所请求域的查询。这样可能会导致应用程序尝试连接至被阻止的站点并通过多个查询迭代重新尝试解析。

   如同 REFUSED 和其他错误响应代码那样，操作系统可能会将递归解析器从其查询任何名称（而不仅仅是被阻止的名称）的名称服务器列表中移除。然而，与通过上述响应代码进行阻止不同，如果阻止时不返回任何响应消息，会带来非常糟糕的最终用户体验，因为应用程序需要等待所有查找超时。这样可能会致使用户改用其他替代递归解析器，例如没有受除名指令或相应阻止策略影响的服务器。

递归解析器的重新配置过程视具体的操作系统而定，但通常需要在“系统首选项”图形用户界面中点击几次鼠标来完成，一般操作系统中提供的许多“应用”级操作系统和类似的智能设备也可一键完成这一过程。在几乎所有情况下，可以说大部分非专业用户都可完成这一重新配置。

正如前文所述，通过递归解析器实施阻止是当前常用的方法；然而，最终用户可使用不实施阻止的递归解析器（例如，接受来自任何来源 IP 地址查询的“开放式”解析器）[16] 或运行他们自己的递归解析器来避开这种形式的阻止。

此外，由于通过递归解析器实现的 DNS 阻止会改写或修改从权威服务器收到的 DNS 响应，因此 DNSSEC 所使用的信任模型链会中断，同时会产生与 DNSSEC 有关的错误。这些错误会使最终用户认为 DNS 递归解析器出现了问题或被攻击。这种想法是有道理的，因为对于 DNSSEC 来说，在技术上无法将按照政府要求而改写的 DNS 响应与发生恶意缓存中毒期间而生成的 DNS 响应相区分。

6. 基于权威服务器或注册管理机构的 DNS 阻止与采用递归解析器的 DNS 阻止之间的对比

某些国家（如英国和美国，前者针对 .uk 顶级域名[17] 中的名称而采取阻止措施，而后者针对 .com 顶极域名 (TLD)[18]中的名称而采取阻止措施）所捕获的域名由在其境内运营的注册管理机构维护。在一些情况下，域名位于注册管理机构的域名保留记录中；但还有一些情况是，修改 DNS 记录以将访问流量重定向至受政府监控的网站。

如果受阻止的域名数量很少，而且创建服务于同一受众或用途的新域名需要一定的成本，域名捕获在阻止互联网内容方面会很有效。由于 TLD 中的阻止是在发布点实施，因此全球所有的 DNS 递归解析器通常会在相对较短的时间内（具体来说是在被阻止的 DNS 记录的 TTL 时间内）将被阻止的域名移除。

如果域名是在注册管理机构层面上捕获的，则 DNSSEC[19]可以继续按预期运行，因为这种操作是在其源头对 DNS 内容的修改，因此，如果正确重新生成 DNSSEC 签名，则 DNSSEC 信任链不会中断。

然而，如果提供要阻止的域名的注册管理机构位于其他法律管辖区，则可能需要不同管辖区的执法或政府官员之间的协作。如果其他国家/地区的法律存在冲突或执法机构没有通过如国际刑警等组织明确司法互助条约、合作协议、配合或协作协议，则可能会存在问题。如此看来，尽管最近以来各执法

[16]常用的开放式解析器包括 OpenDNS (http://www.opendns.com/) 和 Google 公共域名系统 (https://developers.google.com/speed/public-dns/)。

[17]请参见 http://news.techworld.com/personal-tech/3319654/police-take-down-2000-couk-domains-selling-counterfeit-goods/。

[18]请参见 http://en.wikipedia.org/wiki/Operation_In_Our_Sites_v._2.0。

[19]请参见 http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions。

机构之间的配合和协作已有明显改善，但在单一法律管辖区内实施注册管理机构层面上的域名除名仍最为可行。例如，通过多利益相关方 ICANN 程序及在组织中创建特别工作小组来实现协作，如在欧洲刑警组织内创建欧洲网络犯罪中心 (E3C)。[20]

在权威服务器处实施 DNS 阻止，需要每个权威服务器的运营商对其从注册管理机构所收到的区域作出更改，而无需获得该注册管理机构的授权。如果权威服务器由多个组织运营，则可能会带来非常有挑战性的问题。如果一个或多个权威服务器的运营商未能在同一版本的区域数据内进行相同的更改，则对于同一查询将会返回逻辑混乱的结果，具体取决于所查询的解析器、解析器所查询的权威服务器以及查询的时间等等。此外，除非权威服务器正好是区域签名密钥 (ZSK) 的持有者，否则权威服务器运营商对区域所做的修改不会被签名，因而会导致无法对执行校验的服务器进行 DNSSEC 信任链检查。因此，这种形式的阻止可能会不切实际。

采用基于递归解析器的 DNS 阻止可避免这些管辖权的问题，因为除名指令是由发出指令的管辖机构主体下达给其辖区内的 ISP 或其他解析器运营商。但其不利之处在于，由于世界各地的各种网络运营商都会运营递归解析器，因此，不使用协同一致的数据路径过滤及网络负载操作，就不可能确保完全覆盖。此外，在面对端到端应用程序级别的 DNSSEC 验证时，这一过程还会中断 — 下文将对这一内容进行探讨。不过，至少一项研究表明，由于所谓的“上游过滤”现象，在一个国家/地区的 ISP 所执行的用以过滤或阻止内容的操作可能导致内容在另一个国家/地区也被阻止，这是因为 ISP 之间的路径安排所致。[21]这种治外法权的政府影响所带来的意外后果可能会增加所有互联网运营商和用户的运营成本并降低其稳定性。

7. 递归解析器内实施的 DNS 阻止及与 DNSSEC 的冲突

如前文所述，实施 DNSSEC 会对 DNS 阻止活动产生重大影响。DNSSEC 针对 DNS 中数据的真实性问题，从多方面改进了 DNS 协议。尽管支持 DNSSEC 的应用程序目前尚未广泛使用，但对此类应用程序的需求是促使开发和部署 DNSSEC 的一个重大因素。要在当前和未来为安全性敏感的应用程序的加密认证提供支持，则需要端到端部署 DNSSEC — 这对于保护全球互联网中的公众信任度是很有必要的。

通过递归解析器实施的有效 DNS 阻止，与 DNSSEC 的目的和运行相冲突。这是因为，尽管术语“阻止”意味着更改本身是按照法律和或所涉及各方均认可的其他规则而作出的，但是 DNSSEC 的目的就是要确切检测出类似

[20]请参见https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417。

[21]请参见 https://citizenlab.org/2012/07/routing-gone-wild/。

“DNS 阻止”这类操作所作出的更改。“DNS 阻止”所引发的更改与 DNSSEC 所要检测的更改无法区分，如不法分子恶意插入虚假的 DNS 响应，因而导致流量重定向至虚假的服务。对 DNSSEC 签名数据的任何修改与恶意的 DNS 病毒修改看起来没有区别，因为 DNSSEC 中没有特征或信号告诉接受者，所给出的响应已被授权机构而不是域持有者签名。这适用于旨在保留网站的域持有情况，以及旨在显示政府阻止/除名通知以通过重定向替换用户访问的网站的域重定向。在任何一种情形中，最终用户的解析器在验证 DNSSEC 签名的响应时能够报告已发生篡改，但不知道发生篡改的原因。在发现这种篡改时，最终用户的解析器可能会采用各种解决方法，如忽略对从根到权威服务器自身的整个信任链进行反复解析的本地递归解析器。

作为临时的解决方法，在递归解析器一级采用 DNS 阻止是可行的。具体而言，如果是仅在域名持有者或最终用户不使用 DNSSEC 时才阻止或过滤 DNS，则所修改的数据仍被最终用户解析器所接受，并被如 Web 浏览器等应用程序所使用。但是，对于不希望域名被阻止的域持有者来说，解决方法在于对其 DNS 数据进行签名，而对于不希望内容被这种方式阻止的最终用户而言，解决方法是在其存根解析器中启用 DNSSEC。[22] 因此，可将其描述为“临时的权宜之计”。

虽然通常认为 DNSSEC 验证能够或仅能够“在网络中”完成，但这忽略了能识别 DNSSEC 的应用程序的需求。DNSSEC 可“在网络中”用以保护 DNS 缓存不受中毒数据的损害，在早些年的 DNSSEC 部署中，这是互联网行业对 DNSSEC 的唯一用途。然而，DNSSEC 的长远目标在于创建全新类型的、使用基于 DNS 的名称实体验证 (DANE) 等技术的 DNSSEC 最终用户应用程序 — 互联网工程任务组 (IETF) 正在为此努力。[23] DANE 工作组正在努力规范通过 DNSSEC 而不是之前问题缠身的 X.509 证书颁发机构网络来增强安全网络服务器身份验证及浏览器及安全网络服务器之间连接的安全性的机制。[24]

随着将 DNSSEC 作为创建安全应用程序的一般基础架构方面的工作不断推进，可以认为，通过递归解析器实施的 DNS 阻止，要么会对 DNSSEC 部署产生负面影响，要么将在 DNSSEC 得以广泛实施后失效。互联网全球体系要么拥有安全的互联网名称管理，从而确保互联网应用程序的安全性，要么就是通过互联网 DNS 实施有效的内容阻止 — 二者只能取其一。

---

[22]存根解析器是一种小型的 DNS 解析器，它采用递归查询模式将 DNS 解析的大部分工作转移至递归名称服务器。几乎所有的互联网设备都会包含一个存根解析器，且几乎所有的接入网络都会为其客户提供一个递归名称服务器。请参见 http://en.wikipedia.org/wiki/Stub_resolver#Stub_resolvers。

[23]请参见 https://datatracker.ietf.org/wg/dane/charter/。

[24]使用 X.509 最近面临的挑战包括 Diginotar 系统遭受入侵（请参见 http://en.wikipedia.org/wiki/DigiNotar）以及 Comodo 注册机构遭受入侵（请参见 http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/）等多起入侵行为。

8. DNS 阻止的其他意义

除上文所述之外，DNS 阻止和过滤还有其他潜在意义。很明显，这可能涉及到过度阻止及通过使 DNS 路由避开阻止实施点而达到绕开/规避阻止的目的。

8.1 过度阻止

如果采用 DNS 阻止技术，被阻止的实体列表中会有发生错误的风险。这与阻止是基于域名还是 IP 地址或统一资源定位器 (URL) 等其他标识符无关。因此，用来审查某一条目是否应添加到特定列表当中的程序必须安全、可信且广泛征求多方意见。本报告中所列举的阻止示例中使用的列表取自多个来源：私人机构、合作司法机构以及法院或立法机关。SSAC 不去认定哪种过程最佳，而是推荐数种机制来促进技术稳定性：清晰的阻止规则及定义明确的审查和决策流程。

此外，重要的是要认识到：如果阻止针对某一域实施（如 *example.com*），阻止使用该域名系统，不仅会造成访问受阻止 URL *http://example.com/bad-content.html* 下的内容时无法查找域名，还会阻止使用同一域名的所有其他 URL（例如 *http://abc.example.com/* 或*http://example.com/good-content.html*）。DNS 阻止也会阻止所有使用 *example.com* 的同一域和子域的其他服务发出的域名查询，例如电子邮件、网络管理、文件传输等（如 *subdomain.example.com*）。[25]

最后，在任何过滤方案中（无论是 DNS 还是其他），重要的是避免在生成阻止目标方面出错。例如，在数据输入时的一个拼字错误不但会导致无法阻止所要阻止的域名，还会导致无关的域名意外被阻止。国际化的域名 (IDN) 可能会带来一些特殊危险，因为两个国际化域名可能看似一样，但内部却有区别。

8.2 避开实施阻止的国家来路由 DNS 流量

政府用来阻止域名的举措可能会引发最终用户采取一些行动来确保某 DNS 流量能路由至所在国家以外的名称服务器，例如使用 VPN 或特定递归解析器而非网络接入服务商所运营的解析器。这种域名查询的“离岸”路由会将 DNS 的监管和控制转移至其他国家，导致实施阻止的国家打击网络犯罪的行动收效甚微，并会鼓励国外的不法组织开展更多的网络犯罪活动。除了可能发生的额外延时，DNS 流量的外部路由还可能对实施阻止的国家的互联网性能产生影响，因为许多内容传输网络是根据发起查询的解析器的源 IP 地址来决定针对 DNS 查询返回何种信息。对非本地服务器的使用会导致超额的流量在国际链接之中传输。

[25]请参见 http://gigaom.com/europe/orange-censors-all-blogs/，http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/，以及http://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml

如果转移至另一个名称服务器，无论它是同一 ICANN 管理的 DNS 还是一个替代系统，都可以通过修改计算机的配置来实现，这在当今大部分计算机系统上都可以借助图形化用户界面轻松执行。即使对于没有足够的知识来修改计算机或网络 DNS 设置的用户来说，也可以下载到许多可以自动对 DNS 进行修改的脚本和自定义应用程序。例如，在美国移民和海关执法局 开展的“我们网站的行动”早期，便有人提供了 MAFIAA Fire 这一插件。[26]

8.2.1 用户切换解析器所产生的影响

DNS 数据让 ISP 可以了解他们网络上的流量模式和安全威胁。这些信息让 ISP 能识别流量的增加和转移，从而做出业务决策。更为重要的是，DNS 数据的监控有利于网络安全，通常可以让 ISP 诊断拒绝服务式攻击和识别受感染的主机、被攻击的域名以及易受入侵的用户。

如果用户不断抛弃其 ISP 所提供的 DNS 服务器，转而使用其他 DNS 服务器，ISP 将无法应对安全威协并保障网络的高效运作。客户对企业、本地网络运营商或 ISP 所指定的 DNS 服务的弃用，将意味着有更多的受入侵计算机无法识别和修复。此外，客户在致电运营商帮助中心时需要提供的互联网配置属性集更为复杂化，从而增加了成本和故障排查的难度。

上面所述问题还会给 ISP 所在国家的政府带来挑战。这些政府可能会失去通过与网络和互联网服务提供商之间共享数据的方式来获取情报信息的能力，同时缺乏在执法调查当中对重要证据信息的掌握。例如，美国政府可能无法在僵尸网络指令和控制结构以及中毒缓存等方面拥有足够的证据，从而难以开展关闭传播 DNS Changer 这一恶意软件的服务器的“幽灵点击行动”。[27]

用户选择另一国家的 DNS 服务器会带来严竣的执法问题。服务器位于特定执法机构的辖区之外，造成通过法律程序解决问题的能力被削弱。

8.2.2 用户切换解析器对 CDN 本地化的干扰

将 DNS 流量以不符合网络拓扑的方式进行路由（例如通过位于所在国家以外的 DNS 服务器），这一行为也会对网络性能造成负面影响。对于国家而言，会产生额外的传播和往返传输总计时间，而对 ISP 来说其成本也会增加。例如，如果用户通过切换解析器来躲避阻止，则结果可能是 CDN 本地化无法工作，最终用户会被定向至来自托管于国外服务器的 CDN 节点的内容，而非用户拥有直接互联路径的接入网络的内容。

---

[26]请参见 https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/ 和 http://en.wikipedia.org/wiki/MAFIAAFire_Redirector。

[27] 参见 http://www.fbi.gov/news/stories/2011/november/malware_110911。

CDN 通常借助向大范围内的网络上的服务器全局传播相同的内容来实现内容传输的本地化。这一本地化模式减轻了单一服务器的负荷，并将内容从服务器传送至尽量接近用户的位置，从而使网络资源的占用和拥堵现将降至最低。许多 CDN 基于用户 DNS 解析器的 IP 地址来猜测用户的位置。因此，如果用户转用位于国外的 DNS 解析器，CDN 会认为用户是在国外进行浏览。结果，此类 CDN 用户的性能和稳定性都会受影响，并且 ISP 用来传输相关流量的成本也会增加。

9. 结论和更多阅读材料

通过 DNS 来阻止对内容的访问变得越来越多见，人们常将其作为研究和实施的对象。但它也存在一些技术性问题。在 DNS 注册管理机构的层面上实施阻止（直接或通过注册代理商）带来的问题最少，而且这种方式与 DNSSEC 相容，但可能会产生司法问题或触发互联网命名空间的长期割据化。在权威服务器上实施阻止，存在类似的司法管辖问题，但无法与 DNSSEC 相容，因为权威服务器运营商不拥有相同的权力来为包含要阻止名称的区域提供签名。最后，在解析器层面上的实施阻止，这种方式在现今也很常见。如果处理得好，它只是与 DNSSEC 存在一定兼容性问题，但如果处理得不好，则会妨碍 DNSSEC 的部署。

政府和其他机构在部署策略并使用基于 DNS 的阻止或互联网内容过滤时，应考虑到这些问题，并充分理解这些技术影响。

要进一步了解这一主题，可以参阅以下文章：

- *“关闭、暂停、捕获，那么我如何选择！”*，D. Piscitello，http://securityskeptic.typepad.com/the-security-skeptic/2012/08/shutdowns-suspensions-seizures-oh-my.html。
- *“防止访问或删除内容 — 用激光刀还是锯子？”*，D. Piscitello，http://securityskeptic.typepad.com/the-security-skeptic/2012/08/preventing-access-or-removing-content-laser-scalpel-or-saw.html。
- *“采用链锯这种一刀切的方式，无论对于手术还是网络内容阻止都是糟糕的选择”*，D. Piscitello，http://securityskeptic.typepad.com/the-security-skeptic/2012/08/a-chain-saw-is-a-poor-choice-for-surgery-and-for-blocking-content.html。
- *“DNS 阻止中各方利益的平衡”*，P. Vixie, http://www.circleid.com/posts/20110723_alignment_of_interests_in_dns_blocking/。

10. 致谢、利益声明、异议和撤回

以下部分为读者提供有关我们流程的三个方面的信息。“致谢”部分列出为此特定文档做出贡献的成员。“利益声明”部分包括委员会成员的个人介绍，以及本文档材料所暗含的任何真实、明显或潜在的利益冲突。“异议和撤回”部分为各成员提供一个空间来就本文档的内容或制定本文档的流程发表不同看法。

10.1 致谢

委员会感谢以下 SSAC 成员和其他编著者花费时间来撰写和审查本报告。

Alain Aina
JaapAkkerhuis
DonBlumenthal
KCClaffy
DavidConrad
PatrikFältström
JamesGalvin
WarrenKumari
JasonLivingood
Danny McPherson
RamMohan
PaulVixie

10.2 利益声明

以下链接中包含 SSAC 成员的个人简介和利益声明：
http://www.icann.org/en/groups/ssac/biographies-09oct12-en.htm.

10.3 异议和撤回

无异议或撤回要求。