SAC 050
DNS 阻止：利与弊 — 安全与稳定咨询委员会关于在域名系统中阻止顶级域名的报告

ICANN 安全与稳定
咨询委员会
(SSAC) 的
报告
2011 年 6 月 14 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. DNS 阻止：利与弊 4

2. 致谢、利益声明、异议和撤回 5

2.1 致谢 5

2.2 利益声明 6

2.3 异议和撤回 6

1. DNS 阻止：利与弊

对域名系统 (DNS) 的查询响应进行阻止还是变更已成为一个越来越突出的问题。有些组织可能会将域名或互联网协议 (IP) 地址过滤（或其他将防止访问网站内容作为安全策略事务的方式）视为旨在阻止组织内部人员造成电话费用的历史电话控制技术的自然延伸。

用于阻止 DNS 的各种技术手段旨在影响给定管理域名范围内的用户，例如私人或公开运营的网络。虽然利用规避技术可能还是能够连接到目标系统（这包括只通过 IP 地址而不是通过完全限定域名 (FQDN) 来访问站点），但阻止将域名解析到 IP 地址可以防止立即连接到指定的主机。DNS 解析器或网络运营商还可以重写 DNS 响应，以包含映射运营商选择的 IP 地址，无论是重写不存在的域名 (NXDOMAIN) 响应还是重写已有 FQDN 的 DNS 响应，都可能对支持 DNS 安全性扩展 (DNSSEC) 的名称服务器及其用户产生不利影响。一个特别粗糙的方式就是让运营商默默放弃 DNS 响应，尽管这会产生不确定的行为，而且这种做法本身可能也有问题。

无论采用何种机制，实施阻止的组织都应采用以下原则：

1. 组织针对其实施管理控制的网络及其用户施行策略（即，它是策略域的管理员）。

2. 组织确定该策略对其目标和/或其用户的利益有利。

3. 组织使用对其网络运营和用户最不具破坏性的技术来实施该策略，除非法律或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。

如果不应用这些原则，阻止使用 DNS 就会造成更多、更显著的间接损害或意外后果，且无法为受影响的各方提供补救措施。

互联网技术的发展是基于对医学实践中 *primum no nocere*（首先，不要造成损害）— 即要求医疗服务提供者考虑介入治疗可能造成的损害 — 这一基本原则的调整。如果阻止 DNS，且不管是对顶级域名 (TLD)（例如 .example）、二级域名（例如 example.example）还是三级域名（例如 example.example.example）实施阻止，“不要造成损害”都意味着在任何情况下组织策略域之外的互联网用户都不会受到组织策略或其实施的负面影响。

用于 DNS 阻止的所有技术手段，甚至更多用于规避阻止的此类尝试，都会对用户和应用程序的安全性和/或稳定性产生某些影响，还会对全球名称空间的连贯性或全球可解析性产生某些影响。SSAC 无法在所有 TLD 层上划清“有利的 DNS 阻止”

和“有害的 DNS 阻止”之间的界限，尽管委员会可以调查各种阻止方式所产生的、可以观察到的影响，还可以提出一些指导意见用于评估在被阻止的域名之外，哪些阻止方式可能带来最少的意外后果和最小的损害。例如，在最近的一份白皮书中描述了对特定域名或主机名进行 DNS 阻止对 DNS 安全性造成的负面影响。[1]

SSAC 明白 DNS 阻止会伴随 XXX 通用 TLD (gTLD) 添加到根区域中。SSAC 没有足够的信息对此行动表明立场，但委员会希望澄清，无论是在 TLD 还是在次级实施阻止，要将损害降到最低程度，就必须共同努力使组织策略域之外的互联网用户不会因该组织的策略或其实施而受到负面影响。将此基于组织的道德框架延伸到主权国家将需要在 SSAC 现有的基础上进一步了解政治状况。但是我们也可以肯定地说，在国家/地区级别上阻止整个 TLD 会从根本上干预为互联网资源提供单个统一命名系统的目标。如果在没有可将对外部各方的损害降到最低程度的某种正式道德框架的情况下就实施阻止，可能会对更广泛的机构群体带来更多超出预期的负面影响，使希望通过此类阻止来解决的问题更加恶化。此外，在二、三级域名以及 TLD 级别上实施阻止可能会产生替代名称系统和/或根区域，从而造成互联网的不稳定和破坏。

2. 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了贡献的成员。“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。

2.1 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。

KC Claffy
Steve Crocker
Patrik Fältström
Jim Galvin
Warren Kumari
Jason Livingood
Danny McPherson
Ram Mohan
Dave Piscitello
Bruce Tonkin
Paul Vixie

[1] 请参阅 <http://www.redbarn.org/files_redbarn/PROTECT-IP-Technical-Whitepaper-Final.pdf>。

2.2 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/committees/security/biographies-25mar11-en.htm

2.3 异议和撤回

无异议或撤回要求。