CN

SAC 032
关于 DNS 响应修改的初步报告

翻译注释

本文档的原始版本是英文版，可从以下网址获得：
http://www.icann.org/committees/security/sac032.pdf。如果翻译文档与原始文档有出入，或者在理解上有出入，请以原始文档为准。

ICANN
安全和稳定
咨询委员会 (SSAC) 的
咨询报告
2008 年 6 月

引言

DNS 协议[1] 的响应代码 (RCODE) 字段为名称服务器提供了一种方法，使名称服务器在尝试响应客户端（解析器）的查询时可以就遇到的问题发送信号并进行描述。授权名称服务器会返回值为 *名称错误* 的 RCODE 以指示查询的域名不存在。互联网标准也会使用 *域名不存在* 或 *NXDomain 响应* 这两种术语来说明这种错误响应[2]。

只有授权名称服务器发出的“名称错误”响应值才有意义。有些域名注册人会将其授权名称服务委托给内部员工；其他域名注册人会委托外部组织来管理其 DNS。SSAC 称之为委托名称服务代理，或简称为委托代理。DNS 客户端通常不会直接向授权名称服务器发出查询。相反，大部分 DNS 查询都是由叫做 *迭代解析器* 的中间系统来进行解析的。迭代解析器可由任何组织自行操作。也可以由代表客户托管名称服务或为订阅者提供域名解析的服务提供商公开操作。虽然域名注册人与委托代理之间通常会有一些业务往来并且彼此建立了信任关系，但一般来说他们并非与所有迭代解析器运营商都建立了这种关系。因此，我们将在本报告中使用 *第三方* 一词来表示此类名称服务提供商。

在此初步报告中，我们将介绍委托代理或第三方修改 DNS 响应的做法。第一种情况，委托代理接收 DNS 名称查询。委托代理可确定在为域名注册人托管的区域文件中不存在所查询的名称，但返回的 DNS 响应却不会指示 *名称不存在*，相反，返回的响应会指示名称存在，而且会包含一个由代理选择的映射查询名称的 IP 地址。第二种情况，运行迭代解析器的第三方接收由授权名称服务器生成

[1] 请参见 RFC 1035，Domain Name System Implementation and Specification（域名系统实施和规范）(http://rfc.net/rfc1035.html) 以及 IANA registry（IANA 注册机构）(http://www.iana.org/assignments/dns-parameters)
[2] RFC 2308, NXDomain, http://rfc.net/rfc2308.html

的 NXDomain 响应，并以无提示方式更改内容，即，将*名称不存在*响应更改为指示*名称存在*的响应，并插入一个由第三方选择的映射查询名称的 IP 地址。

通过以下几种标签可知存在这种行为：子域重定向、NXDomain 重定向、NXDomain 重写、NXDomain 劫持、子域劫持、错误解析和错误交易。这些标签表明这种做法具有商业意义，但却存在争议。

本报告的目的在于说明 DNS 响应修改对域名注册人、DNS 运营商及互联网用户的影响，并探讨恶意利用这种做法的可能性。本初始报告着重说明对于用户、域名注册人以及依赖“域名不存在”响应来报告错误并进行管理的人群，此做法将带来哪些影响和意外结果。

什么是 DNS 响应修改？

DNS 响应修改是名称服务提供商的一种做法：如果域名注册人的区域信息中未发布所查询的名称，那么名称服务提供商将返回指示*名称存在*的 DNS 响应消息，而不是指示名称不存在的消息。在某些情况下，域名注册人的委托代理会利用域中不存在某个名称的机会（例如，将 www.example.com 错误键入为 ww.example.com），返回*合成响应*，即一个由委托代理选择的映射查询名称的 IP 地址。委托代理可以使用一个通用或默认 IP 地址来映射所有未在区域文件中发布的查询名称：我们称之为*通配符合成。*

而在其他情况下，第三方运行的迭代解析器将对那些它试图代表客户端进行解析的查询的 DNS 响应进行检查。如果发现 DNS 响应包含值为*名称错误*的响应代码，则第三方会将迭代解析器配置为在将 DNS 响应转发给发起查询的客户端之前以无提示方式更改[3]该消息的内容。具体而言，迭代解析器会将响应代码由指示名称不存在更改为指示名称存在。提供商将进一步配置解析器，通过插入映射查询名称的 IP 地址来修改响应内容；需要特别指出的是：此映射不是在域名注册人的区域文件中发布的地址，而是由第三方选择的地址。

在 DNS 注册机构级重定向

SSAC 和互联网架构理事会 (IAB) 以前曾对在 DNS 注册机构级进行重定向和 DNS 合成发表过评论[4], [5], [6]。在本报告中，SSAC 没有提供进一步的评论或建议。但是，为了表述完整，我们在此要对 *TLD 运营商合成响应*的基本流程进行说明：

1) 客户端向迭代解析器 *A* 提交一个要将域名 *example.tld* 解析为 IP 地址的 DNS 查询。

---

[3] 我们将这种行为称为*无提示更改*，这是因为迭代解析器不向客户端或授权名称服务器提供任何明确的协议信息以指示内容已更改。

[4] SAC 006 Redirection in the COM and NET Domains（在 COM 域和 NET 域中的重定向）（2004 年 7 月 9 日），http://www.icann.org/committees/security/ssac-report-09jul04.pdf

[5] SAC 015 Why Top Level Domains Should Not Use Wildcard Resource Records（为什么顶级域不应使用通配符资源记录）（2006 年 11 月 10 日），http://www.icann.org/committees/security/sac015.htm

[6] Tralliance Proposed New Registry Service（SSAC 答复 ICANN 来函，回复：Tralliance 提议的新注册服务），http://www.icann.org/committees/security/sac013.htm

2) 迭代解析器 A 开始解析流程，将该查询转发给根名称服务器。
3) 根名称服务器将返回一份可以解析 *tld* 标签的名称服务器列表。
4) 迭代解析器 *A* 将要解析 *example.tld* 的查询发送给根名称服务器识别到的多个 *tld* 名称服务器之一。

5) *tld* 的名称服务器确定标签 *example* 未能与 *tld* 区域文件中的某个具体标签匹配。*tld* 的名称服务器不会返回响应代码值为 *名称错误* 的 DNS 响应消息；相反，它会撰写一条 DNS 响应消息，将 *example.tld* 解析为它所选择的 IP 地址，并将其返回到迭代解析器 A。

6) 迭代解析器 A 将这条肯定的响应消息转发给发起请求的客户端（也可能会选择缓存此响应）。

委托代理合成的 DNS 响应

在本示例中，我们将介绍委托代理如何对 *example.tld* 的域的 DNS 响应进行合成：

1) 客户端向迭代解析器 *A* 提交一个要将域名 *service.example.tld* 解析为 IP 地址的 DNS 查询。

2) 迭代解析器 A 开始解析流程，将该查询转发给根名称服务器。

3) 根名称服务器将返回一份可以解析 *tld* 标签的名称服务器列表。

4) 迭代解析器 *A* 将要解析 *service.example.tld* 的查询发送给根名称服务器识别到的多个 *tld* 名称服务器之一。

5) *tld* 的名称服务器将返回一份可以解析 *example.tld* 标签的名称服务器列表。

6) 迭代解析器 *A* 继续执行解析流程，将要解析 *service.example.tld* 的查询发给 *tld* 名称服务器识别到的多个 *example.tld* 名称服务器之一。

7) *example.tld* 的名称服务器确定标签 *service* 未能与 *example.tld* 区域文件中的某个具体标签匹配。*example.tld* 的名称服务器会撰写一条 DNS 响应消息，将 *service.example.tld* 解析为在区域文件中定义的一个默认 IP 地址，并将其返回到迭代解析器 A。

8) 迭代解析器 A 将这条肯定的响应消息转发给发起请求的客户端（也可能会选择缓存此响应）。

图 1 对这种形式的 DNS 响应修改进行了图解说明：

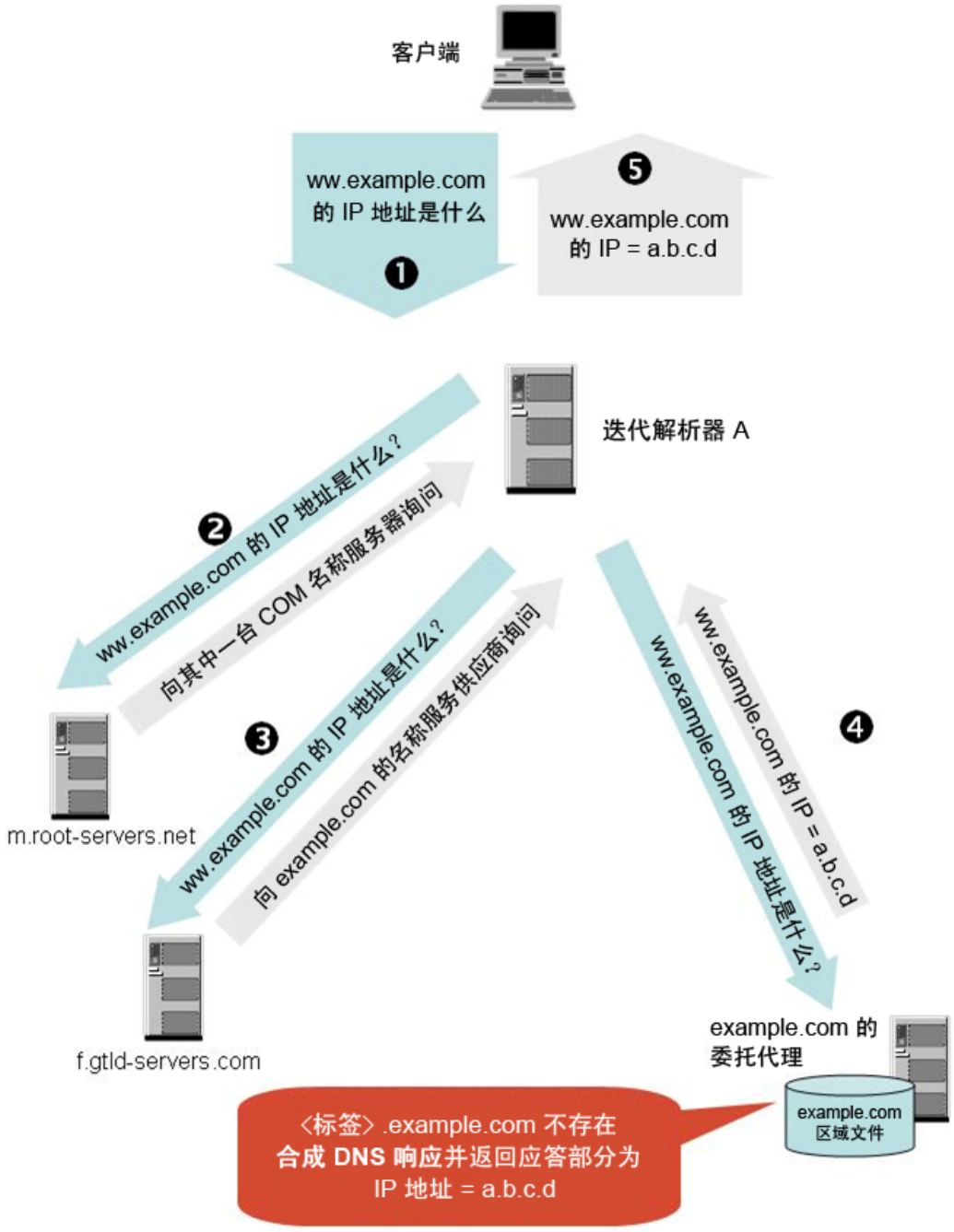

图 1. 由委托代理修改的 NXDomain 响应

第三方 NS 提供商进行的 NXDomain 响应修改

特定名称解析流程所涉及的任何迭代解析器所属的任何第三方名称服务器运营商都可以执行 NXDomain 响应修改。例如：

1) 客户端向迭代解析器 *A* 提交一个要将域名 *service.example.tld* 解析为 IP 地址的 DNS 查询。
2) 迭代解析器 A 开始解析流程，将该查询转发给根名称服务器。
3) 根名称服务器将返回一份可以解析 *tld* 标签的名称服务器列表。
4) 迭代解析器 *A* 将要解析 *service.example.tld* 的查询发送给根名称服务器识别到的多个 *tld* 名称服务器之一。
5) *tld* 的名称服务器将返回一份可以解析 *example.tld* 标签的名称服务器列表。
6) 迭代解析器 *A* 继续执行解析流程，将要解析 *service.example.tld* 的查询发给 *tld* 名称服务器识别到的多个 *example.tld* 名称服务器之一。
7) *Example.tld* 的名称服务器将确定 *example.tld* 区域文件中不包含标签 *service*，然后将响应代码值为 *名称错误* 的 DNS 响应消息返回到迭代解析器 *A*。
8) 迭代解析器 *A* 发现 *example.tld* 的名称服务器已返回一条指示名称不存在的响应消息。迭代解析器 *A* 不会将此响应消息发送给客户端；在将响应转发给客户端之前，它会以无提示方式将 DNS 响应消息中的 RCODE 更改为指示 *名称已找到* 的 RCODE，并插入一个查询应答，将 *service.example.tld* 映射到一个由第三方名称服务器运营商选择的 IP 地址。

值得注意的是，在实践中，无论授权服务器是否返回 NXDOMAIN，解析过程中涉及的任何一方都可以对 *每个* 已确定或被告知不存在的名称执行 NXDOMAIN 重定向。

图 2 对这种形式的 DNS 响应修改进行了图解说明：

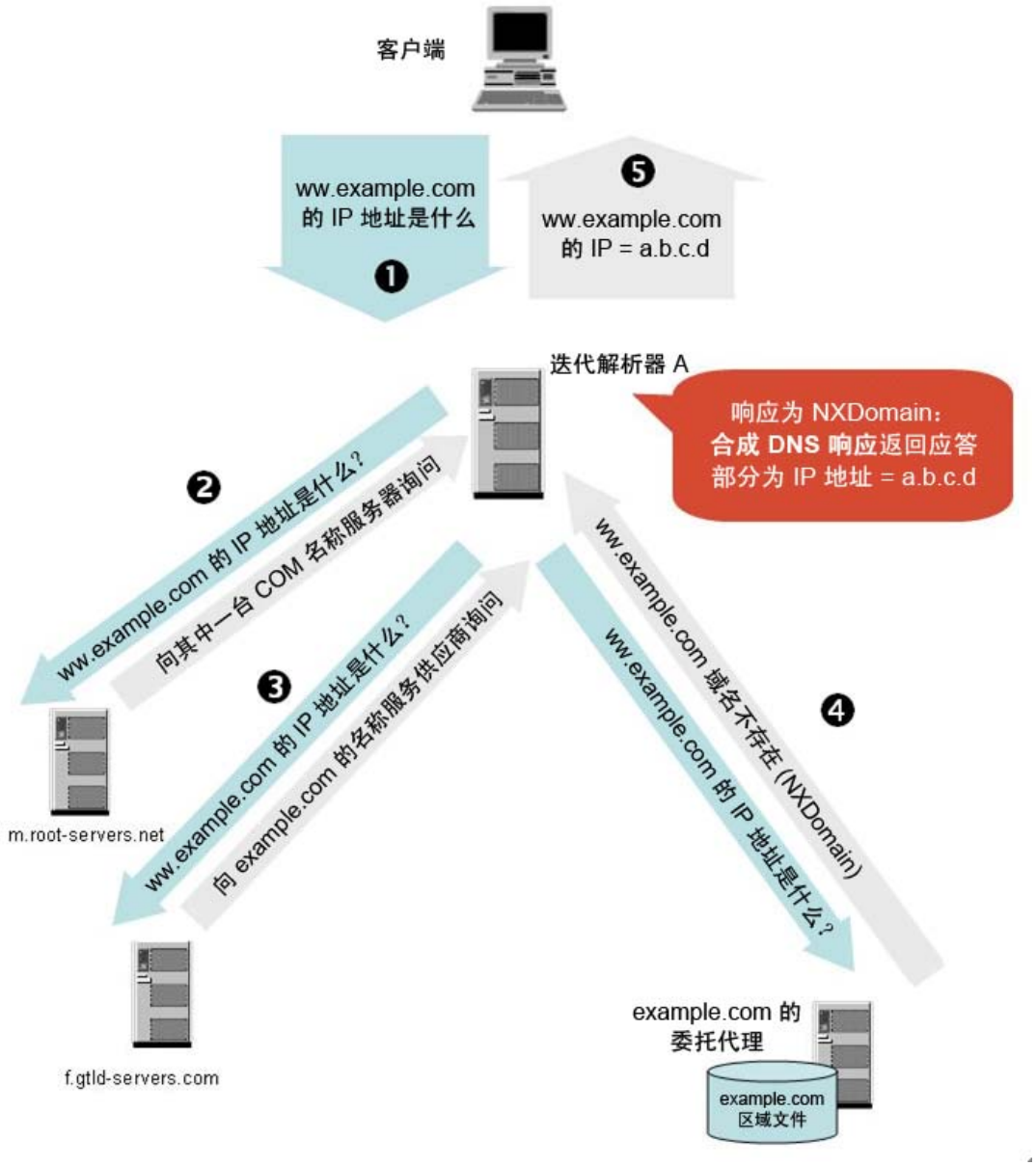

图 1. 由委托代理修改的 NXDomain 响应

谁可以修改 DNS 响应消息？

对于能够重定向 NXDomain 响应消息的几方，上一节中的示例确认了其中的一部分。已经列出的各方包括委托代理和第三方。

委托代理。域名注册人的内部员工可能会作为委托方并管理注册人的区域信息。提供域名的注册服务提供商、互联网服务提供商或外包 DNS 提供商（有偿托管组织的 DNS 的公司）也可能会作为委托方并托管注册人的区域信息。

第三方。任何 DNS 运营商，只要其迭代解析器参与了给定 DNS 查询的解析过程，就能够处理授权名称服务器发给查询发起端的 DNS 响应消息。这些运营商包括：

- 通过以下方式获取收入的公共 DNS 服务提供商：
    - 获得和销售 DNS 流量分析，或
    - 销售发布广告的机会，广告发布在他们插入到更改的 DNS 响应中的地址所托管的页面上
- 为订阅者或（广泛地说）利用 ISP 名称服务的任何一方提供名称解析的 ISP 或 ISP 代理（有偿运行 DNS 用于 ISP 的公司）。
- 提供名称解析和 Web 代理服务的服务提供商。

攻击者也可能为了支持恶意或犯罪活动而修改 DNS 响应。

这份名单还说明了存在多种修改 DNS 响应的动机。我们将在下一节中讨论这些问题。

为什么修改 NXDomain 响应消息？

SSAC 已获悉并已确认各方选择修改 DNS 响应的几种原因。例如，第三方不转发授权名称服务器发出的 NXDomain 响应，而是中途截取并以无提示方式更改 DNS 响应的内容，使该响应包含某网页的 IP 地址，目的是为了：

- **获得收入。**登陆页面在某个域或注册域的子域中托管了广告或其他可创收的内容。
- **增强用户的网络体验。**登陆页面会通知用户（潜在客户）所查询的域名不存在，并会为其提供一种解决这种错误结果的方式，例如，用户可以通过访问登陆页面使用（赞助）搜索形式从错误中恢复。
- **强制执行政策。**登陆页面会通知用户尝试访问的域的页面内容违反了可接受的使用政策。登陆页面可能会识别出特定的内容类型，也可能会提供一份 AUP 副本供用户查看。
- **提供补救培训。**登陆页面会通知用户尝试访问的域已被识别为仿冒域，并且该站点已被暂停。用户可以通过查看登陆页面上发布的反仿冒培训材料，从此次“侥幸脱险”中吸取教训。
- **教唆未授权活动或犯罪活动。**登陆页面以属于该域但未经注册人实例化的某个名称托管可下载的恶意内容以进行犯罪活动（钓鱼、身份盗窃、欺诈等）。

DNS 响应修改是否是安全和稳定问题？

DNS 响应修改有几个特点值得引起注意。SSAC 从参与 DNS 响应修改的委托代理和第三方表现出的行为中注意到以下几点。

1) 委托代理假定代表域名注册人进行操作。从运营的角度来看，委托代理所做的更改可以在 DNS 数据模型中应用。关于是否允许委托代理产生合成响应这一问题，可以通过代理和注册人之间进行协调解决。如果注册人判定某个委托代理不值得信任，则可以选择由其他代理托管自己的区域。
2) 从 DNS 的性质来看，任何提供解析过程所涉及的迭代解析器的第三方都是潜在的中间人，并且能够修改从授权名称服务器接收到的消息，然后再

将这些消息转发给客户端。第三方在解析路径中某个位置修改 NXDomain 响应可能与涉及该注册人的任何业务关系都无关。

3) 为了自身的利益，第三方可以不通知也不征询域名注册人或发起查询的用户的同意，随意更改 DNS 响应的语义和内容。

4) 修改 NXDomain 响应消息的第三方所提供的有关域的信息与域名注册人要分发的信息在几个重大方面有所不同。响应表明标签（子域）已在域内进行实例化，并且映射到特定 IP 地址。但从域名注册人角度来看，此名称并不包含在其区域内。这种响应是错误的，并且曲解了注册人的意图。

5) 第三方通过暗示与域名注册人的关联来影响制定查询的用户的后续行动。如果第三方的目的是为了从所暗示的第三方与域名注册人之间的关系进行受益，则可以证实这是一种欺诈、欺骗或未经授权使用品牌或商标的行为。

6) DNS 响应修改可能会影响非 Web 应用程序，特别是可能破坏电子邮件、互联网电话技术和其他互联网服务。

7) DNS 响应修改可能产生无法预测的响应（虽然名义上是稳定问题，但最糟糕的情况下可能会导致拒绝服务攻击）。

下面我们将介绍这些安全和稳定问题会对域名注册人产生何种影响。

DNS 响应修改对域名注册人有什么影响？

在没有通知域名注册人也未征得其同意就修改 NXDomain 响应的情况下，响应消息无法准确地反映域名注册人预期的域操作状态：

1) 应将区域文件中不存在某名称这种情况报告给查询客户端。具体而言，应该由以无提示方式更改消息的委托代理或第三方将包含响应代码 *名称错误* 的响应返回给客户端，但实际情况却并非如此。

2) 类型 A 资源记录已被写入响应消息的应答部分。但域名注册人发布的区域文件中却没有这种资源记录所描述的名称到地址的映射。

如果仔细检查，就会发现这不仅仅是替代了错误情况的处理方式，而是更改了消息内容。当域名注册人的委托代理创建 DNS 响应消息（无论何种响应）时，代理和注册人都应完全有理由期望中间系统尝试提交未经更改的内容。如果这种假设证明是错误的，那么域名注册人可能会在以下几个方面受到影响：

响应不再传达预期信息。任何依赖 NXDomain 响应做出正确操作或干预的应用或管理活动，都将不再对重定向域内的所有标签起作用。

响应破坏了传统的域信任模式。通常，各个组织都是根据默认的信任模式来判断域是否安全：父域将信任其子域。这种绝对的信任是基于以下假设产生的：在组织域内命名的主机都是由该域的 IT 员工或其指定和信任的代理来管理。修改后的 NXDomain 响应会将用户引向在域名注册人的管理控制和安全域之外运行的主机上进行操作的服务。

响应会对合规测试和审核产生负面影响。执行安全审核的组织，特别是要求执行此审核以证明其合规性的组织，必须将以下情况考虑在内：第三方可能擅自添加主机，这种主机看起来像是采用了该组织域中的名称，但是却不在该组织的管理控制范围之内，并且其名称也不会在组织区域中进行公布。

响应可能引起 DNS 运行不稳定。直接对域的授权名称服务器执行或通过不更改 NXDomain 响应的迭代解析器执行的名称解析，都会返回注册人想要的响应，但相同的查询也可能返回不同的响应，这取决于响应是由修改 NXDomain 响应的第三方进行处理的，还是通过任何可缓存修改后响应的迭代解析器或桩解析器进行处理的。如果域名注册人采用两个委托代理来托管其区域文件，那么也

可能发生这种情况。其中一个委托代理可能公布了其中包含通配符条目的注册人区域文件，而另一个委托代理则可能公布了真实的（未经修改的）区域文件。

与地址映射发生冲突的可能性非常大。域名注册人可能针对某个名称 (ww.example.com) 在其区域文件中添加类型 A 资源记录，这样做的目的只是为了查看第三方（或可能是多方）是否已为该名称映射了一个 IP 地址。
[注意：通常对于客户端请求的任何记录类型而言，都会发生这种情况。]

域中的主机将暴露给任何可通过重定向主机进行利用的漏洞。即使在修改过的 NXDomain 响应中识别的主机是通过合法业务（例如广告或服务促销）运行的，该主机也很容易受到 Web 服务器和 Web 应用程序攻击、跨站点脚本编制或操作系统开发的侵害；尤其是，攻击者可能通过在修改过的 NXDomain 响应中识别的主机将内容插入域名注册人的其中一个系统中。此类攻击并非是理论上的。安全研究员已公开证明通过在修改过的 NXDomain 响应中识别的主机（广告插入服务器）可将脚本插入父域中[7], [8]。

响应会将主机添加到域中，但域名注册人的管理员却无法控制这些站点的内容。在经第三方修改过的 NXDomain 响应中识别的主机可利用域名注册人的商标、名誉、站点和链接广泛度以及搜索引擎的赞助链接协议并从中获益。注册人并不能从此类活动中获得任何好处，而且在某些情况下，还可能会因此类活动而受到伤害。例如，

- 第三方可能在从修改过的 NXDomain 响应中识别的主机上发布广告。这些广告可能会促销域名注册人竞争对手的服务或商品。
- 对于那些在第三方从修改过的 NXDomain 响应中识别的主机上发布广告的公司，将从与域名相关的赞助链接和与注册人业务相关的关键字搜索引擎中受益。
- 注册人可能有自己的广告合作关系，而且发布在第三方从修改过的 NXDomain 响应中识别的主机上的广告服务可能会对域名注册人在其自己 Web 主机上发布的广告产生破坏作用或与之相竞争。这将对域名注册人和广告合作伙伴产生影响，对于注册人而言，其与广告服务合作伙伴的关系将受到危害，而对于广告合作伙伴而言，其增加收入的机会将受到阻碍。
- 第三方从 NXDomain 响应中识别的主机可能发布负面的广告活动或发布旨在损害注册人名誉的错误信息或误导信息。

修改过的 NXDomain 响应不限于类型 A 资源记录。第三方不限于修改将解析假设为 HTTP 连接中所使用主机名的内容的 NXDomain 响应，因为 NXDomain 响

[7] h0h0h0h0，Dan Kaminsky，位于：http://www.doxpara.com/DMK_Neut_toor.ppt

[8] Hacking ISP Error Pages（黑客攻击 ISP 错误页面），Bruce Schneier，位于：http://www.schneier.com/blog/archives/2008/04/hacking_isp_err.html

应可能适合于对任何应用程序中任何资源记录的请求 - DNS 解析器所看到的全部内容是请求中的名称或记录类型。在理论上，第三方通常可以修改任何查询（MX、SRV、NAPTR）的 NXDomain 响应；例如，用于查找 IP 电话号码的 DNS 查询（如返回 NAPTR 资源记录的请求）理论上可以重定向到第三方选择的呼叫服务器。

响应为滥用和攻击创造了机会。可利用伪造响应执行的攻击包括：

- **通过在欺诈子域中注入伪站点进行仿冒。**攻击者可能利用在修改过的 NXDomain 响应中识别的主机上找到的脚本，通过这些脚本攻击域注册人的系统。例如，攻击者可能找到了某个接受输入的脚本，但是却无法验证对该脚本某些参数的输入。攻击者通过在可利用的参数中插入自己的可执行代码，可以将访问者诱骗到站点以执行该站点上的伪造支付或登录表单[9]。攻击者可以应用类似的技术来发布邀请用户下载恶意软件的横幅广告，或者弹出邀请用户更新应用程序或操作系统软件的窗口（但这些更新是恶意的，而并非合法副本）。
- **数据提取。**重定向主机可以采用广告跟踪公司的相同方式，监控流量并收集重定向访问者的网络统计数据。
- **随机 cookie 检索。**重定向主机可以中途拦截域名注册人的 Web 服务器预定发送给客户端的 cookie，并对其进行复制。这可能会导致泄露个人信息、信用卡或帐户凭据。
- **攻击品牌。**许多域名注册人保护品牌和商标的方法是，防御性地在 TLD 下注册带有攻击性、诽谤性、迷惑性的名称或在印刷上类似的名称。攻击者可能会使用通配符插入将相同标签实例化为子域。所有此类名称查询不会返回不存在的域中，而是可能重定向到损坏的网页或存在异议的网页。

除了这些操作和安全影响之外，SSAC 还要指出子域重定向可能引起知识产权和商标问题。这些问题尽管不在 SSAC 的专业范围内，但随着此主题的深入研究可能值得引起合格运营商的注意。

[9] *Exploit Impact and Response（对 XSS 攻击的剖析：使用、影响和回应）*，Russ McRee，ISSA Journal，2008 年 6 月第 12-14 页。

双重修改

可以对 DNS 响应修改本身进行修改。这种现象称为*双重修改*，可以概括如下：

1) 用户 Fred 通过注册服务提供商 *X* 注册了域 *example.tld*。
2) *example.tld* 的注册人使用由注册服务提供商 *X* 提供的 DNS 服务来托管 *example.tld* 的区域文件。
3) Fred 的 PC 使用 *NS1.mylocalisp.tld* 作为其默认的名称服务器。
4) Fred 在 PC1 中打开浏览器窗口，并尝试连接到 *ww.example.tld*。他错误地键入了 *www.example.tld*，这是注册人曾用于通过 HTTP 协议连接其 Web 服务器的地址的主机名。
5) *NS1.mylocalisp.tld* 执行解析 *ww.example.tld* 的过程如下，首先查询根名称服务器找到 *tld*，然后查询 *tld* 的名称服务器找到 *example.tld*，最后查询注册人 X 的名称服务器找到 *ww.example.tld*。
6) 注册机构 X 的名称服务器针对 *ww.example.tld* 返回一个肯定的 DNS 响应，而不是 NXDomain 响应。此响应的应答部分包含类型 A 记录，可将 *ww.example.tld* 映射到 *a.b.c.d*。
7) *NS1.mylocalisp.tld* 会中途拦截注册服务提供商 *X* 的 DNS 响应，并根据之前的 DNS 流量分析将重定向地址 *a.b.c.d* 识别为广告页面。
8) *NS1.mylocalisp.tld* 替换了自己的重定向信息，然后返回应答部分中包含类型 A 记录的肯定 DNS 响应，可将 *ww.example.tld* 映射到 *a.x.y.z*。
9) Fred 在 PC1 中打开浏览器窗口并尝试连接位于 *a.x.y.z* 的 *ww.example.tld*。

初步结论

SSAC 对于 DNS 响应修改做法的初步结论如下。

1) 第三方提供商可通过客户端和域内授权名称服务器之间路径上的任何迭代解析器来修改 NXDomain 响应。委托代理可将通配符条目纳入注册人的区域文件中，并返回该地址映射而不是*名称错误*。

2) 第三方 NXDomain 响应修改重定向给域名注册人带来了很多难以解决的操作和稳定问题，即使通过托管自己名称服务的方式也无济于事。

3) NXDomain 响应修改与合成响应可能会给域名注册人带来安全问题。特别是在父域及其子域之间的信任关系无法得到保证的情况下更是如此。信任关系的破坏可能对安全审核和合规性测试产生负面影响。

4) NXDomain 响应修改与合成响应可能会为恶意攻击域名注册人创造机会，并能够使攻击者有机会利用域名注册人的域资产从事恶意或犯罪活动。

5) NXDomain 响应修改与合成响应可能由修改其所收到的 NXDomain 响应的第三方进行修改。

6) 合成响应的委托代理以及修改 NXDomain 的第三方是已知且可以确认的，而并没有任何不确定性。某些第三方直接实行 NXDomain 响应修改，或通过*错误解析合作伙伴*[10] 进行修改。

7) 委托代理和第三方可能不会清楚明确地公开其实行 DNS 响应修改的事实，即使公开了这一事实，也不会揭示这种做法可能会对域名注册人的利益造成负面影响。某些提供商声明他们将按照服务协议中的条款行使执行错误解析或重定向的权力，但实际却不给注册人任何退出选择以另外挑选其他提供商的机会。

8) NXDomain 响应不仅显示了来自域名注册人的错误情况，而且还传达了与区域文件中的条目相关的内容。该内容应与任何其他应用程序内容同等对待。

[10] 参加此次活动的某些人士确认，每年由错误交易造成的损失超过十亿美元 http://barefruit.com/services.htm

9) 响应修改的影响力超出了网络应用程序的范围。特别是通过互联网服务在电子邮件和语音中执行替换和插入操作，仍然是可以从事类似操作的新领域。

10) DNS 响应修改可能会引起知识产权和商标问题。

初步建议

SSAC 提出了以下几条初步建议。

1) SSAC 以前曾多次针对在 TLD 级别合成 DNS 响应提出建议。同时建议不应在子域级别执行类似的操作。

2) 注册人可以通过业务往来关系及信任关系，来控制委托代理如何对区域文件中不存在名称的查询的进行回应。具体而言，注册人应指定其授权名称服务器是返回“名称错误”，还是返回合成响应。

3) 注册人应问明其委托代理如何对待注册人未注册的子域。SSAC 同意 IAB 的观点并提出如下建议：委托代理在未向域名注册人说明本报告和其他资料中所确定的风险时，不应在区域中使用 DNS 通配符；委托代理在未经注册人知情同意的情况下不应生成通配符与合成响应；委托代理应提供选择退出机制，允许客户端接收其查询对应的原始 DNS 回应。

4) 第三方应公开其实行 NXDomain 响应修改的事实，并为客户提供退出选择的机会。

5) 那些依赖准确的 NXDomain 报告来实现运营稳定的组织应选择在服务条款中声明不会修改 DNS 响应的委托代理。

6) 注册人应研究如何对不存在的子域提供端到端的鉴定验证，如 DNSSEC 安全扩展[11], [12], [13], [14]。组织应通过选择值得信赖的迭代解析器提供方来进一步尝试降低 NXDomain 响应修改的暴露级别，进而避免组织客户端的查询由那些可能会实行子域重定向的不受法律限制的名称解析提供商进行路由。

---

[11] RFC 4033 DNS Security Introduction and Requirements（DNS 安全性介绍和要求），http://rfc.net/rfc4033.html

[12] RFC 4034 Resource Records for DNS Security Extensions（DNS 安全扩展的资源记录），http://rfc.net/rfc4034.html

[13] RFC 4035 Protocol Modifications for DNS Security Extensions（DNS 安全扩展的协议修改），http://rfc.net/rfc4035.html

[14] RFC 5155 DNS Security (DNSSEC) Hashed Authenticated Denial of Existence（DNS 安全 (DNSSEC) 哈希认证否定存在），http://rfc.net/rfc5155.html

今后的工作

子域重定向对于商业、经济、安全和运营的影响特别值得注意。据我们所知，DNS 响应修改似乎主要限制在基于 Web 的应用程序的范围内，至于它对其他基于 IP 的服务会产生哪些影响的问题还值得进一步研究。SSAC 鼓励社群考虑将负面响应变成创收机会的广泛意义，而不考虑运营结果，也不考虑注册人和 DNS 数据客户端的愿望。从根本上说，错误解析和“错误交易”这样的做法将不定性和可变性引入了传统的错误管理模型和信任模型，从而开了令人烦恼的先例。我们不清楚这些做法是否会扩展到电子邮件服务、语音服务和协作服务，甚至扩展到寻址、路由和其他互联网核心操作；我们也不清楚这些做法对基于 IP 的通信的影响程度有多严重。