供 IT 专业人士使用的域名冲突识别与缓解指南

2014 年 8 月 1 日
版本 1.1

目录

1.简介

在全球域名系统 (DNS) 根中输入新的顶级域名后，组织可能会发现，用于解析特定于其网络的部分“内部”域名的查询会返回不同的值，因而为用户和程序提供不同的结果。存在以下两个基本问题：渗入到全球互联网的“内部”域名，以及私营域名空间被确定为与全球域名系统域名空间存在冲突。

导致这种不同结果的原因是，网络管理员本想要使用内部域名空间在本地解析域名系统查询，而现在使用全球域名系统中的新顶级域名数据进行解析。在这种情况下，预计从不离开内部网络的查询现在可以在全球域名系统中获取结果，因此，这些结果会有所不同。渗漏的域名会导致不同的结果，至少会为用户带来麻烦（例如，它们可能会导致对网页的访问产生延迟）。另外，它们可能还会引发安全性问题（例如，电子邮件发送到错误的接收方）。

本文档介绍的缓和及预防策略适用于各类组织最广泛使用的私营域名空间类型。本文档介绍了内部域名渗入到全球域名系统时，组织可能遇到的问题，并给出建议的缓和办法。下面给出的说明和建议面向 IT 人士（网络管理员、系统管理员和 IT 部门员工），他们通常了解域名系统的工作原理以及自己内部域名系统的工作原理。如需更多背景知识，读者可以参阅本文档附录 A。关注安全性的读者可以专门参阅 ICANN 安全与稳定咨询委员会 (SSAC) 提供的报告。

ICANN 是管理全球域名系统根的组织，在咨询了域名空间主题专家后编写了本文档，旨在为私营域名空间可能与全球域名系统根发生冲突的组织提供帮助。ICANN 还发布了其他文档，其中介绍了全球域名系统的组织方式、向域名系统根添加新域名的方式等内容。本文档附录 A 列出了许多主题的参考，可供读者进一步阅读。此外，ICANN 最近开始帮助使用私营域名空间的组织了解其域名空间开始出现冲突的时间；该内容在第 1.4 节和第 6 节加以介绍。

请注意，尽管本文档介绍域名冲突方面的缓和措施，但只是讨论组织在解析域名时可能会遇到的问题，而不讨论与全球域名系统本身操作相关的其他问题。例如，全球域名系统的根域名服务器始终会陷入全球域名系统从来不会处理的查询中（请参阅附录 A 中的 *SAC 045*），但根域名服务器的配置一直足够良好，可以应对这些过量的查询。本文档不介绍与根域名服务器相关的问题，只论述当查询意外渗漏到全球域名系统根域名服务器时所带来的后果。

ICANN 开发了一个网页，其中包含与域名冲突相关的信息材料，网址为：http://www.icann.org/namecollision。该网页还介绍了一个流程，用于报告因新通用顶级域名 (gTLD) 引起域名冲突而产生的严重损害。

1.1 域名冲突

全球域名系统是层级域名空间，域名系统中的域名包括一个或多个构成全名的标签。层级顶部是域名系统根域，包括一组诸如 com、ru、asia 等域名；这些域名是全球 TLD（顶级域名），通常简称为“TLD”。例如，www.ourcompany.com 可能就是一个完全域名（通常称为*完全合格域名*或 *FQDN*）。

几乎所有私营域名空间也是层级结构。私营域名空间有三种主要类型：

- **从全球域名系统分支出来的域名空间** – 从全球域名系统分支出来的私营域名空间以可在全球域名系统中解析的域名为基础，但该域名下的整个目录结构都在本地管理，并且包含 IT 管理员从来不会在全球域名系统中看到的域名。例如，以 winserve.ourcompany.com 为基础的私营域名空间：该私营域名空间 (winserve) 中的域名由私营域名服务器管理，并且在全球域名系统中不可见。

- **将自身的根与私营顶级域名结合使用的域名空间** – 私营域名空间的根是一个标签，而该标签不是全球顶级域名。整个目录结构（包括私营顶级域名的目录结构）由在全球域名系统中不可见的私营域名服务器进行管理。例如，如果私营域名空间以 ourcompany 为基础，则私营域名服务器也负责 www.ourcompany、region1.ourcompany、www.region1.ourcompany 等。许多不同类型的域名空间将自身的根与私营顶级域名结合使用。例如，Microsoft 的 Active Directory（在部分配置中）、多播域名系统(RFC 6762)，以及仍在互联网的某些位置使用的旧版 LAN 目录服务。

- **通过使用搜索列表创建的域名空间** – 搜索列表是本地域名解析程序（用于私营域名空间的解析程序或全球域名系统递归解析程序）的一项功能。使用搜索列表时，用户可以为了方便而输入更简短的域名；解析期间，域名服务器会在查询中的域名右侧附加配置的域名。（这些配置的域名也称为*后缀*。）

从全球域名系统分支出来的域名空间只有在与搜索列表结合使用时才会引起域名冲突。如果 FQDN 来自全球域名系统，则包含该 FQDN 的所有查询从定义上来说不会与全球域名系统中的其他域名存在域名冲突。此类查询只有在通过使用搜索列表意外创建域名时才会导致域名冲突。

“私营域名空间”的概念使许多人感到困惑，这些人在很大程度上已经习惯于典型的互联网用法，也就是说，他们只熟悉全球域名系统命名，在得知发出用于解析域名的某些请求后不会或应当不会对全球域名系统进行查询时可能会感到惊讶。在得知对域名的某些查询特意在私营域名空间中开始而在全球域名系统中结束时，甚至会感到更为惊讶。出现域名冲突的其中一个可能的原因是，针对私营域名空间的域名服务器的查询错误地在全球域名系统中开始。

1.2 私营顶级域名导致的域名冲突

域名冲突会因两类事件引发。第一类事件是，针对私营顶级域名下的一个完全合格的根域名的查询从私营网络渗漏到全球域名系统中。第二类事件是，在全球域名系统中查询时，结果与私营顶级域名下存在的私营网络域名完全相同。

出现此类域名冲突的常见原因是，使用了类似 Microsoft Active Directory 等系统中的域名，而该域名在配置系统时不是全球域名系统中的顶级域名，但在后来该域名添加到了全球域名系统中。此类域名冲突在以前已经出现过许多次，随着在全球域名系统中引入新顶级域名，这类冲突还会继续出现（请参阅附录 A 中的*新通用顶级域名项目简介*）。

1.3 搜索列表导致的域名冲突

导致域名冲突的另一个原因是处理搜索列表。如果查询不是 FQDN，它便是*简短无限定域名*。搜索列表包含一个或多个后缀。这些后缀会迭代附加到查询右侧。如果解析程序无法解析简短无限定域名，它便会从列表中附加后缀来尝试解析该域名，直到找到匹配的域名。搜索列表是一项很有用的功能；但在处理搜索列表时会使用不是 FQDN 的简短无限定域名，因此会意外创建不在全球域名系统中的根域名空间。在这种情况下，当用户本打算用作简短无限定域名的字符串却由搜索列表来完成并且解析为 FQDN 时，会发生域名冲突。

例如，假定域名解析程序有一个搜索列表，其中包含 ourcompany.com 和 marketing.ourcompany.com 后缀。另外，假定用户在使用该解析程序的程序中输入 www。这样，解析程序可能会先查找 www，如果未返回结果，随后可能会查找 www.ourcompany.com 和 www.marketing.ourcompany.com。

请注意本例中使用的词语“可能”。因为在不同的操作系统或应用程序中，解析域名时搜索列表的使用规则会有所不同。有些系统总是在应用搜索列表前先尝试在私营域名空间或全球域名系统中解析域名。然而，有些系统却在要搜索的字符串不包含“.”字符时先使用搜索列表。有些系统会在要搜索的字符串以“.”字符结尾时使用搜索列表。有些操作系统和应用程序（例如，Web 浏览器）的搜索列表规则已经更改了多次。因此，无法预测何时使用或不使用搜索列表以及域名是否为简短无限定域名，进而也就无法预测简短无限定域名是否有可能会渗漏到全球域名系统中。请参阅附录 A 中的*新通用顶级域名问题：无点域名和域名冲突*，以了解搜索列表处理多样性的详细信息。

上面描述的搜索列表可能会令某些读者感到惊讶，因为它们随处可见，乍一看似乎不会形成“私营域名空间”。搜索列表中的每个后缀定义一个在解析域名时可能会查询的其他域名空间。这就形成了一个私营域名空间，其仅在客户端使用特定解析程序查询该域名空间时才能可靠地工作。根据搜索列表的实施情况，有些域名解析程序甚至可能会在附加搜索列表中的任一域名前先尝试用户输入的或者是在软件中配置的简短无限定域名。例如，如果在互联网上的某个位置键入 www.hr，域名系统解析程序可能会生成一种结果，而在另一个位置键入该词可能会产生另一种结果。出现这种情况时，其中一个域名空间相对于另一个域名空间便是“私营”。

不通过全球域名系统解析 FQDN，而是使用搜索列表会导致域名解析不确定。搜索列表引起的域名冲突很难预测，因为搜索列表极为常见。它们是在许多操作系统、网络设备、服务器中安装的域名解析程序软件的一部分。解析程序软件在不同系统之间、相同操作系统的各种版本之间的表现会有所不同，甚至可作为从网络上发出请求的操作系统或应用程序的一项功能。为了避免出现这种不确定性和不可预测的结果，最好部署一种域名解析服务，使其仅使用全球域名系统来解析域名。

1.4 协助检测新通用顶级域名中的域名冲突

从 2014 年 8 月 18 日开始，通用顶级域名获得域名系统根域的授权后，需要使用该通用顶级域名来进行为期 90 天的*受控中断*服务。在受控中断期间，将从新通用顶级域名的权威性域名服务器发送针对各种域名系统查询的易于识别的答案。这些答案用于警告将面临域名冲突的组织，它们需要立即采取措施防止因查询渗漏而可能出现的损害。

此外，从这一天开始，在授权某些二级域名进入全球域名系统之前，需要使用一些已经位于根域中的通用顶级域名来进行为期 90 天的受控中断服务。其目的与上述目的相同：也是为了警告私营查询处于渗漏状态的组织，它们需要尽快缓和可能面临的损害。

请注意，这些规则仅适用于通用顶级域名，而不适用于针对国家和地区代码的顶级域名（通常称为“ccTLD”）。将国家和地区代码顶级域名添加到根域后，其运营商可以选择采用受控中断，但并不强制要求这样做。

2.域名冲突引起的问题

如果查询从私营网络渗漏到全球域名系统，则基于这些查询的域名冲突会导致多种意外结果。如果查询获得正面响应，但其答案来自全球域名系统而非预期的私营域名空间，则创建该查询的应用程序将尝试连接到非私营网络中的系统，并且可能会成功。此类连接可能属于一种骚扰行为（在解析域名时造成延迟）。但也可能是安全性问题，即可能产生恶意漏洞，具体取决于应用程序在连接后所执行的操作。

2.1 定向到非预期网站

假定用户在使用私营网络时在其 Web 浏览器中输入 https://finance.ourcompany，并且该网络具有一个私营顶级域名为 ourcompany 的域名空间。如果该浏览器对域名 finance.ourcompany 的查询按预期进行解析，浏览器将获得财务部内部 Web 服务器的 IP 地址。不过，假定顶级域名 ourcompany 也是全球域名系统的组成部分，并且该顶级域名具有二级域名 (SLD) finance。如果查询渗漏，它将解析为其他 IP 地址，而不是在私营域名空间中解析该查询时的地址。现在，假设这个其他 IP 地址托管着一台 Web 服务器。浏览器将尝试连接到公共互联网而非私营网络上的 Web 服务器。

如前所述，即使在没有私营顶级域名的网络中，也会出现相同的问题，但使用搜索列表却不会。假定某个浏览器通常用在以下网络上：用户使用的搜索列表含有域名 ourcompany.com，并且用户输入域名 www.finance 才能转到主机 www.finance.ourcompany.com。现在，假设某位员工正在咖啡厅从移动设备上使用该浏览器。如果该查询渗漏到互联网，并且有一个名为 finance 的顶级域名，则该查询可解析为不同的 IP 地址，例如，在全球域名系统中的域名为 www.finance 的完全不同的主机。该查询将导致浏览器尝试连接到公共互联网上完全不同部分的 Web 服务器，而不是在查询转到私营网络上的解析程序时的服务器。

对于该情景，用户通常会认为这是错误的网站，并且会立即退出。但是，如果浏览器“信任”Web 服务器，那么它可以向该服务器提供大量信息，因为其域名与浏览器此前访问的域名相同。该浏览器可能会自动输入登录数据或其他敏感数据，这样便可在组织外捕获或分析该信息。在其他情况下（例如，对组织精心策划的攻击），该浏览器可能会连接到托管恶意代码的站点，该恶意代码可在计算机上安装危险程序。

请注意，使用 TLS 和数字证书可能并不会有助于防止因域名冲突而带来的危害；实际上，这会让用户误认为很安全，情况可能会更为糟糕。许多针对全球域名系统中的域名颁发证书的数字证书认证机构 (CA) 也会针对私营地址空间中的简短无限定域名颁发证书，因此，被错误定向到某个站点的用户可能仍会看到有效的证书。有关私营域名空间中的域名证书的详细信息，请参阅附录 A 中的 *SAC 057*。

2.2 将电子邮件定向到错误的收件人

域名冲突可能引发的结果并不局限于 Web 浏览器。如果收件人地址中的主机名相同，原本发送给某个收件人的电子邮件可能会发送给另一个收件人；例如，如果 ourcompany 变成全球域名系统中的顶级域名，则发送给 chris@support.ourcompany 的电子邮件可能会转发给另一个完全不同的用户帐户。即使消息未发送给特定的电子邮件用户，可能也会尝试发送，这种尝试会使电子邮件内容可在组织外进行捕获或分析。

许多网络设备（例如，防火墙、路由器，甚至打印机）可能已配置为通过电子邮件发送通知或日志数据。如果输入的要接收电子邮件通知的收件人姓名后来受到全球域名系统中域名冲突的影响，该通知可能会

发送给完全意想不到的收件人。消息正文中包含的可能会披露网络配置和主机行为的事件或日志数据有可能会泄漏给非预期收件人。如果此类数据的预期收件人一直收不到日志数据，IT 员工执行的常规网络性能或流量分析可能会中断，或者无法调查或缓和可触发通知的事件。

2.3 安全性降低

如果出现的域名冲突未得到缓和，可能会使私营网络中的系统出现意外行为或受到损害。依赖域名解析才能正常运行的系统以及同时还执行安全功能的系统*可以*在使用 FQDN 时可靠地执行并且可从全球域名系统中解析出来。

例如，在防火墙中，安全规则通常基于数据包流的源和目标。数据包的源和目标为 IPv4 或 IPv6 地址，但许多防火墙也允许将其作为域名输入。如果使用简短无限定域名，并且未按预期进行域名解析，则这些规则可能无法像管理员预想的那样来阻止或允许网络流量。同样，防火墙日志通常使用域名，如果使用的是简短无限定域名，而这类域名通常以不可预测的方式解析，则可能会对事件监控、分析或响应造成干扰。例如，审查日志的 IT 员工可能会误解事件的严重性，因为日志中的简短无限定域名可能会标识不同的主机，具体取决于日志的创建位置（即，在日志中，同一个简短无限定域名可能看起来与两个或更多个不同的 IP 地址相关联）。由于大部分防火墙可以充当其自身的域名系统解析程序，或者允许管理员使用或配置搜索列表，因此可能会使该问题得到缓解。

2.4 受域名冲突影响的系统

应当对所有与网络连接的系统进行检查，确定其是使用基于私营顶级域名的主机名，还是使用基于搜索列表的主机名。所有这些“使用”实例将需要更新为使用全球域名系统中的 FQDN。要检查的系统或应用程序的大致列表将包括：

- **浏览器** – Web 浏览器允许用户指定 HTTP 代理的位置，这些代理在私营网络上极为常见。检查用户或 IT 员工是否创建了自定义主页、书签或搜索引擎：它们包含指向私营网络上的服务器的链接。有些浏览器还包含一些配置选项，可用于指定在何处获取有关 SSL/TLS 证书的吊销信息，它们可能指向私营网络上的主机名。

- **Web 服务器** – Web 服务器提供的 HTML 内容可能包括嵌入了主机名的链接和元数据。检查私营网络上的 Web 服务器是否包含具有简短无限定域名的内容。检查 Web 服务器的配置文件是否包含私营网络上其他主机的简短无限定域名。

- **电子邮件用户代理** – Outlook 和 Thunderbird 等电子邮件客户端都包含一些配置选项，可用于指定在何处使用 POP 或 IMAP 协议接收电子邮件，以及在何处通过 SUBMIT 协议发送电子邮件；所有这些内容可能都会使用私营网络上的主机名。检查这些应用程序是否配置为从分配了简短无限定域名的主机获取有关 SSL/TLS 证书的吊销信息。

- **电子邮件服务器** – 检查电子邮件服务器中是否有一些配置列出了其他本地主机的简短无限定域名，例如，备份电子邮件网关、脱机存储服务器等。

- **证书** – 检查使用 X.509 证书的应用程序（例如，电话和即时通讯程序）是否含有一些配置数据使用简短无限定域名来确定在何处获取 SSL/TLS 证书的吊销信息。

- **其他应用程序** – 自定义应用程序可包含许多可能会用来存储主机名的配置参数。最明显的空间会出现在配置文件中，但主机名可能会出现在各种应用程序数据中、社交媒体或 Wiki 站点的链接中，甚至以源代码进行硬编码。检查这些配置数据是否含有简短无限定域名。

- **网络设备** – 检查网络基础设施设备 – 防火墙、安全信息和事件管理 (SIEM) 系统、路由器、交换机、网络监控设备、入侵检测或预防系统、VPN 服务器、DNS 服务器、DHCP 服务器、日志服务器 – 确定这些设备是否配置了私营网络上其他设备的简短无限定域名。

- **客户端管理** – 检查集中式客户端管理工具（例如，用于配置组织工作站和网络设备的工具）的由系统控制和重置的配置（特别是搜索列表）中是否含有简短无限定域名。

- **移动设备** – 手机和笔记本电脑等消费者设备可能有一些配置选项与上述应用程序的配置选项类似，因此，可能有一些配置选项包含本地网络中的简短无限定域名。

应当对上述所有系统中用于存储简短无限定域名的配置数据进行检查，以确保在私营域名空间的根发生更改时或者不再使用搜索列表时可以更改这些域名。

3.缓和域名冲突的时间

有时，域名会添加到全球域名系统根域，例如，国家/地区名称发生更改时，或者 ICANN 授权新的顶级域名时。在超过二十年的时间内，几乎每年都会添加两种顶级域名。2013 年和 2014 年添加了新的顶级域名，可以确定的是未来几年将添加更多顶级域名。

过去的经验表明，在向域名系统添加顶级域名时，会出现一些域名冲突。过去的经验还表明，私营域名空间中的域名已经渗漏了许多年，在某些情况下，渗漏频率极其高；有关详细信息，请参阅附录 A 中的 *SAC 045*。用于私营网络的域名空间和域名解析从来没有像管理员想象的那样彻底分离，并且管理员希望由内部域名服务器解析的域名查询有时却会发送到全球域名系统中的解析程序，这也是经过历史验证的。

网络管理员有时根据假设来选择域名，即假设全球域名系统的根中的域名列表不变，而实际上该列表已随着时间发生了改变并且还将变化。例如，对于捷克斯洛伐克，cs 顶级域名大约是在 25 年前添加的；许多大学使用的搜索列表允许用户输入以 cs 结尾的域名表示计算机科学系，这在大学域名内是完全合格的域名，这些决定导致在向根域添加新顶级域名时域名解析不确定，因为以 cs 结尾的域名现在是全球域名系统中的 FQDN。即使在当前全球域名系统根域名通常不会与私营域名空间（私营顶级域名或搜索列表）中的域名重叠时，网络管理员通常也会忘记使域名位于全球域名系统根中的私营域名空间保持最新。

建议 IT 部门尽快开始进行缓和工作。采取“我们将使防火墙更好”的立场可能会减少某些冲突，但决不会根除所有冲突。同样，声明“我们将让我们的用户务必使用我们的域名服务器”或“我们将使远程工作人员使用 VPN”可能会减少某些冲突，但这样可能还会使其余冲突更难以诊断。

不管域名中的字符如何，都会发生域名冲突；但是，在私营顶级域名中使用 ä、中 和 й 等非 ASCII 字符会使冲突分析变复杂。解析程序可能会以难以预测的方式发出查询，可能与互联网的标准不符，因此，确定域名冲突的发生时间变得困难得多。

尽管全球域名系统根的结尾比过去几年大，但向根添加域名也极为常见。对于要添加的每个新顶级域名，都有可能与通常在未注意的情况下已经渗漏到互联网的私营域名空间发生域名冲突。组织已经使用域名并承担冲突风险许多年。

请注意，对于已经在其网络中使用全球域名系统中的 FQDN 的组织来说，向域名系统根添加新域名不是问题，并且以后也不会成为问题。这些组织将发现其对域名系统下的域名的使用不会发生任何变化，因为不存在域名冲突。只有使用私营顶级域名的组织，或者使用的搜索列表允许输入简短无限定域名，而缩短后的域名本身可能是全球域名系统中的有效域名的组织，才会出现冲突问题。

3.1 确定出现冲突的可能性

为了确定您所在组织的私营域名空间是否与其他域名空间存在域名冲突，您需要确定组织使用的所有私营域名空间和域名系统搜索列表并将其编成目录，然后以这些源编译顶级域名列表。对于大部分组织而言，通常只有一个仅包含一个顶级域名的域名空间，但是有些组织，特别是与其他也使用私营域名空间的组织合并的组织（例如，由于商业合并或并购）具有多个私营顶级域名。

接着，需要确定全球域名系统区域的当前及预期内容。全球域名系统的当前根域中的域名位于以下位置：http://data.iana.org/TLD/tlds-alpha-by-domain.txt。要确定是否考虑通过当前新通用顶级域名项目对私营域名空间中的域名进行分配：

1. 请转到 https://gtldresult.icann.org/application-result/applicationstatus
2. 单击“字符串”列中的箭头
3. 滚动浏览各个页面，直到找到包含您的私营域名空间域名的范围

如果刚创建的私营顶级域名列表与域名系统区域中的域名列表之间存在重叠，可能会出现域名冲突，因此需要立即进行缓和。

请注意，将当前一轮新顶级域名输入到根域中后，可以提议更多顶级域名；尤其是新顶级域名列表可能会发生更改，私营域名空间与未来的新顶级域名之间可能会发生域名冲突。此外，私营顶级域名包含两个字母（例如 ab）的组织应当注意，两个字母的顶级域名会预留作国家/地区代码，这些域名将通过完全不同的程序添加到根域中。

3.2 授权被无限延迟的全球域名系统通用顶级域名

ICANN 声称将无限延迟对三个顶级域名的授权：.corp、.home 和 .mail。这些通用顶级域名在私营域名空间中仍然很常用，因此，冲突风险明显高于其他顶级域名。这种延迟并不保证是永久延迟，因此，使用这三个域名之一作为私营域名空间的所有组织都应遵守第 4 节或第 5 节中有关从私营域名空间迁移的说明。但是，相对于使用的域名预期以后会在全球域名系统根中出现的组织，使用这三个域名之一的组织有更多时间来执行迁移。

4.缓和与私营顶级域名相关的问题的步骤

数十年来，一直建议最好不要使用私营顶级域名。实际上，多年来，Microsoft 的 Active Directory 和服务器产品中提供的说明一直明确劝阻使用私营顶级域名。如果域名以私营顶级域名结尾，由于该域名渗漏到全球域名系统而导致域名冲突，缓和这类域名冲突最有效的做法是从使用私营顶级域名改为使用以全球域名系统为基础的顶级域名。

本节中所述步骤适用的网络具有以下特点：因自身原因而选择使用私营顶级域名作为其根，并使用搜索列表来解析简短无限定域名，而不是以全球域名系统作为其域名空间的根并查询全球域名系统来解析 FQDN。本节适用于所有采用私营顶级域名的组织，而不仅限于已将域名查询渗漏到全球互联网的组织。如果您所在组织使用的是您认为“安全”的私营顶级域名，也就是说，该域名尚未有人申请或尚未得到批准可授权进入全球域名系统根，这种情况下，您仍需认真考虑更改为以全球域名系统为基础的域名。如果您就职于一个大型组织，该组织使用多个私营顶级域名（例如，已与其他公司合并而未合并其两个域名空间的公司），则必须对每个私营顶级域名执行本节中所述的步骤。

很可能是在组织选择使用私营顶级域名时，考虑采用了特定的命名规范。此处所述的步骤可能与原始模型存在冲突。对于因私营顶级域名而导致的域名冲突，为了可靠地缓和与这些冲突相关的问题，用户和系统都需要更改域名的使用方式，本地域名服务器需要重新配置，这可能会让某些用户感觉不方便。对可能会影响您所在组织的意外或不良结果加以解释可提高认知，并让您的用户社群能够顺利接受。

重要说明：在您执行本节中所述步骤的同时，您可能还需要缓和因搜索列表导致的域名冲突，这将在第 5 节中进行介绍。第 5 节中的许多步骤与本节相同，可以同时执行。

4.1.监控进入权威性域名服务器的请求

为了缓和与私营顶级域名相关的问题，需要列出在任何请求中使用当前私营顶级域名的所有计算机、网络设备以及所有其他系统。更改所使用的域名时，自动使用旧私营域名的所有设备都将需要更新。

要对系统进行这种监控和列举，可以使用以下三种常见的方法：

- 权威性域名服务器（例如，Active Directory）可能具有记录功能。启用记录功能可以收集有关私营域名的所有查询的详细信息。
- 许多现代防火墙也可以配置为检测和记录私营域名的查询。这可能没有通过命名系统本身进行记录那样有效，具体情况取决于您的网络拓扑。例如，如果某个查询没有通过防火墙，防火墙就无法检测到该查询，因此会将其遗漏。
- 如果上述二个方法均不可使用，则可以使用数据包捕获程序（如 Wireshark）监控和收集发送到权威性域名服务器的流量以及从该服务器发出的流量。但是，此方法需要使用某种程序对捕获到的数据进行处理，才能发现仅针对私营域名的查询。

有些组织将会（并且应当）选择执行比上述更多的操作，以增加找到所有请求的几率。请注意，此步骤可能会产生令人困惑的结果。计算机和手机等设备具有可供用户键入域名的应用程序；这些设备都将作为调查对象，即便可能没有存储任何旧私营域名版本也是如此。对于此步骤，只需要知道您的网络中所有存储旧私营域名的位置以及应用程序所使用旧私营域名的位置。

4.2.创建自动使用私营顶级域名的各个系统的清单

您需要从上一步骤获得日志数据汇总。该汇总文件应当列出所有设备和被查询的所有域名，而不是创建查询的设备的各个实例。需要列出所有被查询域名的原因是，有些设备具有多个应用程序，而每个应用程序都需要进行修复。因此，该汇总文件必须包含所有系统以及各个系统上使用私营顶级域名的所有应用程序。该汇总文件便成了需要更改的设备的清单。

4.3.确定全球域名系统域名的管理位置

您可能已经获得组织的全球域名系统域名，域名可用于私营域名空间的根。您需要确定域名系统域名的负责人员以及他们用来创建和更新域名系统域名的流程。这可以由 IT 部门完成，也可以通过服务提供商（通常是您获取互联网连接的公司）完成。

4.4.将私营域名空间的根更改为使用全球域名系统中的域名

在使用全球域名系统域名作为私营域名空间的根时，一种常见的策略是使从全球域名系统授权的域名可供公众访问，然后使用现有权威性域名服务器来管理其下的所有域名。例如，如果您的公司使用全球域名 ourcompany.com，您可能会选择 ad1.ourcompany.com 作为根域名。

如果您的组织使用全球域名系统中的多个域名，您应当使您的域名以可供组织中的 IT 员工能够最轻松地进行控制的域名为基础。在某些情况下，其他域名由其他实体（比如市场营销部门）加以控制。如有可能，最好以 IT 组织已经控制的域名作为您域名的基础。

进行此类更改所需的步骤取决于所使用的私营域名服务器软件、该软件的具体版本、私营网络上域名服务器的拓扑，以及域名服务器的现有配置。这些详细信息超出了本文档的论述范围，但在当前系统的供应商说明中应有相应信息。此外，在许多组织中，此类更改还要求从一定的管理级别进行授权，尤其是在全球域名系统域名的管理不同于私营域名空间的管理时，更是如此。

在此步骤中，如果您使用的证书针对使用私营域名空间中域名的主机，则您需要为使用新（完全合格）域名的主机创建证书。获取这些证书的步骤取决于您的 CA，因此也超出了本文档的论述范围。

4.5.必要时为主机分配新 IP 地址

如果您的 TLS 证书基于旧的私营顶级域名，您将需要为新域名获取新证书。如果 Web 服务器不支持 TLS 的服务器域名指示 (SNI) 扩展（即允许在同一 IP 地址的 TLS 下提供多个域名），将需要向主机添加 IP 地址，使主机支持原始 IP 地址上的旧私营域名以及新 IP 地址上的新域名。另外，您也可以将 Web 服务器软件更新为可以正确处理 SNI 扩展的版本。

4.6.创建一种用于监控新旧私营域名是否对等的系统

将所有私营域名更改为使用新根后，您应继续提供地址服务并记录旧私营域名的查询，以便检查未更新为使用基于域名系统的域名且不在清单中的系统。因此，您需要确保新私营域名和旧私营域名的 IP 地址具有相同的值。

有些私营域名空间软件可用于并行显示两个树状图，但如果软件较旧或者具有多个权威性域名服务器，您可能需要使用自定义工具来监控对等性。这些自定义工具通常需要查询新域名空间和旧域名空间中的

所有域名，如果出现不一致，将向您发出警告，以便您确定哪个系统发生了更改，而另一个系统中没有同时进行更改。

如果因为具有 SSL/TLS 证书而需要在上一步中添加 IP 地址，对等监控软件应当允许存在不一致。

4.7.培训用户和系统管理员使用新域名

除了更改在配置中输入域名的系统外，还需要改变用户的想法，使他们从使用旧私营域名改为使用新私营域名。应在执行以下步骤前先完成该培训，这样，用户便有机会熟悉新域名，但通过培训应使用户明确：更改即将出现，他们应当开始思考新域名。这也是培训用户使用 FQDN 的好时机。为了提高用户认知并使其能够顺利接受，需要对可能会影响您所在组织的意外或不良结果加以解释。

4.8.将所有受影响的系统更改为使用新域名

本步骤是让网络中的所有系统（个人计算机、网络设备、打印机等等）真正实现从旧私营域名迁移到新私营域名的关键。私营域名应以系统为单位逐个由新域名系统域名取代。在系统上的所有软件中找到旧私营域名的每个实例，并将其替换为新域名系统域名。同时，您应当反对使用搜索列表中的简短无限定域名。

之前开始的监控在此步骤中极为重要。您可能无法确定嵌入了旧私营域名的所有系统中的所有应用程序。但是，在每个系统发生更改后，都需要查询监控系统，以便了解该系统是否仍在请求旧私营域名。

很多系统在首次启动时都会运行一些初始化应用程序。这些应用程序中可能嵌入了系统域名，很难找出所有这些域名。将系统中的所有域名从旧私营域名更改为新域名系统域名后，重新启动系统并使用监控软件检测域名查找。如果系统在查找任何旧私营域名，您需要确定发起该请求的软件，并将其更改为使用新域名。此过程可能需要数次重启系统，才能正确地完成系统配置。

4.9.在域名服务器上开始监控旧私营域名的使用情况

应该对权威性域名服务器进行配置，以开始监控所有对具有旧根的域名的请求。由于用户不应再使用这些域名，所以该监控步骤创建的日志可能不会太大；如果是这样，您需要对网络上的特定系统重复执行上述某些步骤。

4.10.在外围设置长期监控以检测旧私营域名

采用前面的步骤应该找到了绝大部分使用旧私营域名的情况，但少数（可能是关键）系统可能仍在使用旧私营域名，不过可能只是极少数。检测这些域名查询的一种方法是，将规则添加到您网络边界上的所有防火墙中，以便查找任何遗漏的请求。这些规则应该具有高优先级，而且应该配置为能够生成事件通知，以便 IT 员工能够及时获知。您也可以选择在防火墙日志中查找这些事件，但这样做极有可能造成遗漏。请求发生时触发的警告可使工作人员检测出目前这些可能仅为极少出现的事件。有些防火墙需要支付额外的费用添加额外的功能才能支持此类规则；如果您的防火墙是这样，那么您就需要评估找到遗漏的请求所获得的益处是否值得花费额外的费用。

4.11.将旧根中的所有域名改为指向不起作用的地址

用户经过培训后，确保他们在旧私营域名被移除前便停止使用的最有效的方式是，使所有旧私营域名指向一个服务器，而您已将该服务器配置为对所有类型的服务请求均无响应。这还有助于将仍在使用旧域名空间，但在先前的步骤中未检测到的所有系统排除。

所指向的地址应该是保证不运行任何服务的服务器。这样做的结果是，任何使用旧私营域名的系统都将收到错误的信息，应用程序也会报告用户可以很容易检测到的或可以理解的错误；在意识培训期间，您可以建议用户向 IT 员工报告此类型的所有错误。执行此步骤时，用于检查旧域名与新域名对等性的监控系统（如前文所述）需要在发生更改时立即进行更新。

这些域名每次应更改一个，两次更改或两批更改之间至少应间隔几个小时。此步骤可能会呼叫 IT 部门，因此，使更改分阶段进行将有助于平衡呼叫负载，因为仍在使用中的域名会开始停止工作。

4.12.如果为使用旧私营域名的任何主机颁发了证书，请将其撤销

如果您的组织为网络中使用旧私营域名的任何服务器颁发了 SSL/TLS 证书，应将这些证书撤销。如果您的组织充当自身的 CA，此操作非常容易。如果使用商业 CA 为私营域名空间颁发证书，您需要确定 CA 请求撤销的流程；不同的 CA 可能对此类请求具有不同的要求。

4.13.新域名的长期运营

请注意，旧私营域名及其下方的域仍会提供服务，只要您运行域名服务器，它们便会一直提供服务。没有将其删除的理由，在 Active Directory 等许多系统中，很难将系统中配置的第一个域名删除。

留下该域名实际上有一个很好的理由：这可以让您了解网络上系统中的旧私营域名是否存在任何残留痕迹。只要与该私营顶级域名下的所有域名相关的所有地址指向未运行服务的主机，您就可以使用域名服务器中的日志（以及一个额外的益处：记录该服务器所有流量的系统日志）来确定在删除旧私营域名时的全面程度。

5.缓和与搜索列表相关的域名冲突的步骤

为了可靠地缓和因搜索列表导致的域名冲突相关问题，用户和系统需要更改其使用域名的方式。通过更改通知、认知程序和培训的方式，有助于让用户提前做好准备。

请注意，如果您已采用集中管理，那么这些操作或许没有像想象中那样困难。很多经常使用搜索列表的人都知道，他们在需要时还可以键入完整的域名（例如，如果他们正在从组织的私营网络外部访问服务器时），相比那些仅了解简短无限定域名的人，培训这些人将会轻松一些。

5.1.监控进入域名服务器的请求

为了缓和因搜索列表导致的问题，您需要了解在任何请求中使用搜索列表的所有计算机、网络设备和任何其他系统。需要更新所有自动使用搜索列表的设备。

要对系统进行这种监控和列举，可以使用以下三种常见的方法：

- 递归域名服务器（例如 Active Directory）可能具有日志记录功能，您可以开启日志记录功能，以获取所有使用简短无限定域名的查询详情。
- 许多现代防火墙也可以配置为检测并记录对所有域名的查询。这可能没有通过命名系统本身进行记录那样有效，具体情况取决于您的网络拓扑。例如，如果某个查询没有通过防火墙，防火墙就无法检测到该查询，因此会将其遗漏。
- 如果上述二个方法均不可使用，则可以使用数据包捕获程序（如 Wireshark）监控域名服务器。但是，此方法需要使用某种程序对捕获到的数据进行处理，才能发现仅针对简短无限定域名的查询。

请注意，此步骤可能会产生令人困惑的结果。计算机和手机等设备都有可供用户键入域名的应用程序；这些设备都将作为调查对象，即便可能没有存储任何简短无限定域名也是如此。对于此步骤，只需要知道您的网络中所有存储简短无限定域名的位置以及应用程序所使用简短无限定域名的位置。

5.2.创建自动使用简短无限定域名的各个系统的清单

您需要从上一步骤获得日志汇总。此汇总文件应当列出所有设备和被查询的简短无限定域名，而不是创建查询的设备的各个实例。需要列出所有被查询域名的原因是，有些设备包含多个需要修复的应用程序。该汇总文件便成了需要更改的设备的清单。

5.3.培训用户和系统管理员使用 FQDN

除了更改可在任何配置（系统级配置或单个应用程序的配置）中输入简短无限定域名的系统外，您还需要改变用户的想法，以便让他们从使用简短无限定域名转变为使用完整域名。还应对会影响您所在组织的意外或不良后果进行解释，以便提高意识并巩固接受度。

5.4.将所有受影响的系统更改为使用 FQDN

按系统使用同等的 FQDN 逐个替换简短无限定域名。系统上所有软件中的每个简短无限定域名的实例均需被替换为完全合格域名。

之前开始的监控在此步骤中极为重要。您可能无法确定所有被更改且内嵌简短无限定域名的系统中的所有应用程序。但是，在每个系统发生更改后，都需要查询监控系统，以便了解该系统是否仍在请求简短无限定域名。

很多系统在首次启动时都会运行一些初始化应用程序。这些应用程序可能嵌入了依靠搜索列表的系统域名，查找所有这些域名可能很困难。将系统中的所有域名更改为使用 FQDN 后，重启系统并使用监控软件来监测域名查找。如果系统正在查找任何简短无限定域名，您需要确定发起该请求的软件，并将其更改为使用 FQDN。此过程可能需要数次重启系统，才能正确地完成系统配置。

5.5.关闭共享域名解析器上的搜索列表

本步骤是让网络中的所有系统（个人计算机、网络设备、打印机等等）真正实现从简短无限定域名迁移到完全合格域名的关键。搜索列表可以存在于任何能进行域名解析或能为其他系统提供配置的系统中，如 DHCP 服务器。这些系统通常为独立的域名服务器，但也可能是防火墙或其他网络设备。不管系统类型如何，都需要关闭各个系统的搜索列表，以防止用户在给定的域名空间中使用简短无限定域名。

5.6.在域名服务器上开始监控简短无限定域名的使用情况

应该对域名服务器进行配置，以开始监控所有对需要使用搜索列表的域名的请求。如果您提供提前通知和培训，您的用户就不得再使用这些域名，这样此监控步骤创建的日志不会很大；如果是这样，您可能需要对您网络上的特定系统重复执行上述某些步骤。

5.7.在外围设置长期监控以监测简短无限定域名

采用前面的步骤应该已经找到了绝大多数使用旧私营域名的情况，但是少数（可能是关键）系统可能仍在使用简短无限定域名，即便可能只有很少一部分。检测这些域名查询的最佳方法是，将规则添加到您网络边界上的所有防火墙中，以便查找任何遗漏的请求。这些规则应该具有高优先级，而且应该配置为能够生成事件通知，以便 IT 员工能够及时获知。您也可以选择在防火墙日志中查找这些事件，但这样做极有可能造成遗漏。请求发生时触发的警告可使工作人员检测出目前这些可能仅为极少出现的事件。有些防火墙需要支付额外的费用添加额外的功能才能支持此类规则；如果您的防火墙是这样，那么您就需要评估找到遗漏的请求所获得的益处是否值得花费额外的费用。

6.检测新通用顶级域名中的域名冲突

自 2014 年 8 月 18 日起，ICANN 将要求根域中新获授权的通用顶级域名协助组织检测其何时将对新顶级域名中域名的请求泄漏至全球域名系统。此协助将持续 90 天，新通用顶级域名在前期数天内很有可能位于根域中；之后，新通用顶级域名将与根域中其他顶级域名的表现一样。此协助通过本章中描述的“受控中断”服务提供。

显然，需要缓和其私营域名空间和全球域名系统之间域名冲突的组织在相应的新顶级域名进入根域前应该做的就是：不应等待 90 天。（这对于选择两个字母作为其顶级域名的组织尤其如此，因为这些域名无需执行受控中断。）受控中断是对组织的最后警告，在顶级域名开始为查询提供“真实”回复前，组织需要迅速执行缓和措施。

本章描述如何在权威性域名服务器上执行受控中断，以及它如何出现在对查询的回复中。它也为拥有私营域名空间的组织提供建议，以确定组织观察到的操作性更改是否是由于受控中断导致的，如果是，如何去处理那些更改。

6.1 受控中断说明

对于在 2014 年 8 月 18 日之后添加至根域的新通用顶级域名，ICANN 要求为其提供受控中断服务，此服务专用于中断其对私营域名空间中域名的请求泄漏至全球域名系统的设备。目前，当此类域名系统请求泄漏至全球域名系统时，根域名服务器返回带有编码的响应，指示该域不存在。（从技术角度上讲，这是被设置为数值 3 的响应标题的 RCODE 字段，被默认定义为“NXDOMAIN”响应。）

在受控域服务期间，响应中没有 NXDOMAIN 错误，不包含针对错误的错误指示，但包含发送请求的系统最有可能通知的数据。无法设计出一种可以始终获得通知的响应，因为许多不同类型的软件都可以发起域名系统请求；然而，在充分记录错误的系统上，以及网络管理员可观察域名系统流量的网络上，可观察到 ICANN 要求的受控中断。

以受控中断方式操作的通用顶级域名将以可预测的方式响应多种多样的域名系统请求。第 6.2 节说明如何观察获取针对这些域名系统查询的受控中断响应的系统行为。

- 到目前为止，最常见的域名系统查询是针对 A 记录，即与域名相关的 IPv4 地址。那些查询将始终返回 IPv4 地址：127.0.53.53。此地址为发送查询的主机回路地址，因此，如果应用程序使用该地址启动任何类型的联系，它将返回此消息。当然，这可能会失败，因为几乎所有进行域名系统查询的程序均要使用此地址来响应，以联系另一个服务器。

- 另一个常见的域名系统请求针对包含文字的记录，通常称为“TXT 记录”。在受控中断服务中，TXT 记录响应将始终为该字符串“您的域名系统配置需要及时关注，请参阅 https://icann.org/namecollision”。显示此类文字记录的系统为观察员提供关于域名冲突的信息。

- 对于针对邮件服务器的域名系统请求（从技术角度上讲，针对的是邮件交换器或 MX 记录），受控中断服务会将包含“your-dns-needs-immediate-attention.<TLD>”的域名作为响应，其中“<TLD>”为域名系统请求中的顶级域名。此域名可能出现在邮件客户端或邮件服务器的错误响应中。查找包含“your-dns-needs-immediate-attention.<TLD>”的域名的地址时，将返回 127.0.53.53。

- 受控中断服务将包含“your-dns-needs-immediate-attention.<TLD>”的域名作为对服务 (SRV) 记录查询的响应。对 SRV 记录的查询不如那些对 IPv4 地址、文本记录和邮件服务器域名的查询那样常见，但对即时消息和语音传输等较新应用程序的查询却越来越常见。

于 2014 年 8 月 18 日之前添加至根域的通用顶级域名也可能拥有受控中断服务，用于顶级域名中可能二级域名的子集。这些域名的受控中断中返回的记录与以上所述记录相同。ICANN 要求阻止某些二级域名进入顶级域名，这些二级域名可能会在 90 天受控中断期结束后处于活动状态。

6.2 观察受控中断

请务必注意，收到受控中断响应的应用程序，其表现并不一定会与它在受控中断前的表现有明显不同。然而，应用程序的表现很可能会有所不同，这种不同很可能是由于故障造成的；希望该故障会提供相关的错误消息，该应用程序用户应将此消息报告给负责处理此事的系统管理员。如果错误消息含有 IPv4 地址 127.0.53.53，则有充分的迹象表明该错误是由于程序使用了从私营域名空间泄漏到公共互联网的域名。

这是因为当之前针对查询获得 NXDOMAIN 响应的程序开始获得实际响应时，出现受控中断服务，所以导致错误发生。当然，当新通用顶级域名采用实际数据响应时，这些错误稍后才会出现，受控中断服务可能会按照 ICANN 的要求仅持续 90 天。在此期间，错误将会更加明显，因为错误消息包含 IPv4 地址 127.0.53.53、文字“您的域名系统配置需要及时关注，请参阅 https://icann.org/namecollision”，或者含有“your-dns-needs-immediate-attention”的域名。

如果网络管理员正在积极搜索那些含有响应的域名系统消息，则在组织的网络上也会出现受控中断。可以在适当的入口点通过网络分流器完成此类搜索，也可以在防火墙上完成此类搜索。不必依靠查看受影响计算机中的错误消息来进行此类观察；相反，网络管理员可以确定哪台计算机其对私营域名空间中域名的请求正从组织的网络中泄漏。

无论通过何种方式发现受控中断，结果都应该是收到受控中断响应的计算机应被重新配置，从而仅对组织的域名服务器（而非全球域名系统）进行域名系统查询。即使这种设置通常是操作系统的一部分，但还没有标准的方法来指定此类设置。如果计算机从组织网络中的服务器（通常称为“DHCP 服务器”）获取其网络设置，则需要更改该服务器设置，从而使域名系统查询进入组织的域名服务器，而非全球域名系统。

若观察到一台计算机收到了受控中断响应，则表明该组织网络上的其他计算机也可能收到了受控中断响应。即使那些计算机未显示任何表明其收到受控中断响应的迹象，系统管理员也应立即查看同一网络上所有计算机的域名系统设置。切记受控中断仅持续 90 天，因此只有有限的时间来查找域名系统设置错误的计算机。

当然，进行此类更改仅能临时缓和域名冲突的潜在问题。本文档的第 4 节和第 5 节提供关于如何执行永久缓和的说明。

7.总结

域名冲突有可能会给使用私营域名空间的企业和组织带来无法预料的后果。本文档列出了一些潜在后果，并给出了改变在企业和组织内部使用私营域名空间方式的最佳实践。本文档还描述了受控中断是确定域名冲突的影响在何处会变得比较明显的一种方式。

在域名空间下，若一个私营顶级域名正在成为（或已经成为）一个全球域名系统下的顶级域名，则最佳缓和措施为将该域名空间迁移至全球域名系统下的一个根域。对于使用搜索清单下的简写域名的域名空间来说，其缓解措施是不再使用搜索清单。推行这些缓解措施还需要长期监控私营网络，确保停止使用所有可能导致域名冲突的情况。随着某些新顶级域名获得授权进入根域，组织可通过某些方法判断何时将出现域名冲突。

解决域名冲突的一个全面缓解措施是，在任何使用域名的情况下都采用完全合格的域名 (FQDN)。对于已经使用全球域名系统的网络来说，这意味着不再使用搜索列表。对于使用私营域名空间的网络来说，这意味着该私营域名空间应属于全球域名系统的一个根域，且不得使用搜索列表。

附录 A：更多阅读资料

以下文档由 ICANN 内部的各个组织编撰而成。其他组织也提供了一些有用的文档。最重要的是，您的域名服务器软件和/或硬件的供应商在其技术支持网站上可能会提供宝贵的信息。

A.1.新通用顶级域名项目的介绍：

本页面介绍了将数百个新通用顶级域名添加到全球域名系统中的计划的历史、实施和进展情况。
http://newgtlds.icann.org/en/about/program

A.2.域名系统中的域名冲突

ICANN 委任 Interisle Consulting Group, LLC 撰写这份关于潜在域名冲突的深度报告。报告中简要介绍了域名冲突，列出了当前在根服务器中查询的不存在的顶级域名的数据，还提供了大量有关域名冲突可能产生的问题的背景信息。
http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf

A.3.新通用顶级域名冲突事件管理规划

该规划已被 ICANN 采纳，用于管理新通用顶级域名和私营域名空间之间发生的域名冲突事件。其中还包括很多对 ICANN 收到的早期关于根域中域名冲突相关提案的意见的回应。
http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf

A.4.域名冲突事件管理框架

本文档是新通用顶级域名冲突事件管理规划的一个组成部分。它说明了用于自 2014 年 8 月 18 日起获得授权进入域名系统根域的通用顶级域名的受控中断服务细节。
http://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf

A.5.新通用顶级域名问题：无点域名和域名冲突

根据被查询的简短无限定域名中的内容，不同系统上的搜索列表可以产生千差万别的结果。本文档虽然重点探讨无点域名（顶点上有地址记录的顶级域名）的搜索列表，但在很多其他文档中也提供了有关搜索列表处理的宝贵信息。
https://labs.ripe.net/Members/gih/dotless-names

A.6.SAC 045：根级域名系统中的无效顶级域名查询

本 ICANN SSAC 报告描述了在撰写时根服务器中出现的顶级域名查询的类型。
http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

A.7.SAC 057：SSAC 针对内部域名证书问题所提出的建议

本 ICANN SSAC 报告描述了包含私营（内部）域名的证书的安全性和稳定性含义。报告中指出了 CA 的一种实践，该实践可能会被攻击者利用并给安全互联网通信的隐私和完整性带来极大的风险。
http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf