2023 年 5 月草案

公告：遵守《注册服务机构认证协议》和《注册管理机构协议》中的 DNS 滥用义务

本公告就如何解释和遵守《注册服务机构认证协议 (Registrar Accreditation Agreement, RAA)》和《通用顶级域 (Generic Top-Level Domain, gTLD) 注册管理机构基本协议 (Registry Agreement, RA)》有关域名系统 (Domain Name System, DNS) 滥用缓和义务的 [日期] 修订案（简称“DNS 滥用修订案”）提供了指导。

除非“DNS 滥用修订案”进行了特别修改，否则在这些修订案之前生效的所有 RAA 和 RA 义务仍然适用并有效。

对于本公告中未定义的所有大写术语，RAA 和 RA 中已指定其含义。

采用本公告中所述做法的注册服务机构和注册管理机构可能会履行“DNS 滥用修订案”中规定的义务，但遵循其中一种或多种做法并不会自动认定注册服务机构或注册管理运行机构已履行其义务。下面所述的示例仅用于说明目的，而并非旨在对可能采取的缓和措施加以限制。无论在何种情况下，只要 ICANN 合同合规部发起调查，注册服务机构和注册管理运行机构就必须提供证据，证明其遵守了相关的 RAA 和 RA 要求。

背景介绍

ICANN 组织与注册管理机构签订合同，根据 RA 运营 gTLD。RA 规定了注册管理运行机构的职责，包括维护 gTLD 中所有注册域名的权威数据库以及发布 gTLD 的 DNS 区。

ICANN 还与各注册服务机构签订 RAA，该协议允许注册服务机构在 gTLD 内提供域名注册服务。RAA 概述了注册服务机构的职责，

例如核实注册人（或注册域名持有人）信息以及维护准确记录。注册服务机构和注册管理机构的职责和义务有所不同，分别反映在其各自的协议中，即 RAA 和 RA。

ICANN 有权执行 RAA 和 RA 中规定的与域名注册服务和域名有关的规则。本公告重点介绍了 gTLD 中被用作 DNS 滥用工具或机制的域名（或注册域名）。RAA 和 RA 中的“DNS 滥用修订案”要求基于注册服务机构和注册管理运行机构分别可以采取的措施，以尽量减少 DNS 滥用造成的损害及受害的范围和强度。这些要求还考虑到注册服务机构和注册管理运行机构只代表 DNS 生态系统的一部分，DNS 生态系统还包含许多参与方[1]。根据 DNS 滥用事件的具体情况，检测、评估、验证和阻止滥用活动的最合适参与方可能会有所不同，有时可能是注册服务机构或注册管理运行机构之外的参与方。

DNS 滥用

就 RAA、RA 和本公告而言，“*DNS 滥用*”是指恶意软件、僵尸网络、网络钓鱼、网址嫁接和垃圾邮件（当垃圾邮件被用作其他四种 DNS 滥用类型中的任何一种的传递机制时），这些术语在《安全与稳定咨询委员会关于 DNS 中应对滥用问题的互用方案的报告》(SAC 115[2]) 的第 2.1 节中进行了定义：

> **恶意软件**是一种未经用户同意而在一台设备上安装和/或执行的恶意软件，它破坏了这台设备的运行、收集敏感信息，和/或获得对私人计算机系统的访问权限。恶意软件包括：病毒、间谍软件、勒索软件和其他不需要的软件。
>
> **僵尸网络**是一组连接了互联网的计算机集合遭到恶意软件的感染，并被命令在一名远程攻击者的控制下执行活动。

[1] 有关更多信息，请参阅 FIRST 的 DNS 滥用特殊利益团体编制的报告，该报告还包含为安全事件响应团队提供的建议，说明在不同的安全事件响应阶段可以就不同的 DNS 滥用技术与哪些组织联系。
此外，互联网与管辖权政策网络 (https://www.internetjurisdiction.net/) 在其“运营方法、规范、标准和机制”中针对这些形式的 DNS 滥用提供了进一步指导。

[2] ICANN 安全与稳定咨询委员会的 SAC 115 第 2.1 节，第 12 – 13 页，2021 年 3 月 19 日

网络钓鱼在以下情况下发生：攻击者通过发送欺诈性或外观相似的电子邮件、或引诱最终用户使用仿冒网站，来欺骗受害者，使其泄露敏感的个人、企业或财务信息（例如：账号、登录凭证、密码等等）。一些网络钓鱼攻击活动旨在说服用户安装恶意软件。

网址嫁接通常通过 DNS 劫持或投毒，将未知用户重定向到欺诈性网站或服务。当攻击者使用恶意软件将受害者重定向到犯罪者的网站，而不是最初请求的网站时，就发生了 DNS 劫持。DNS 投毒会导致 DNS 服务器（或解析器）以带有恶意软件的虚假互联网协议地址进行响应。网络钓鱼与网址嫁接不同，网址嫁接涉及修改 DNS 条目，而网络钓鱼则是欺骗用户输入个人信息。

垃圾邮件是未经请求的批量电子邮件，收件人并未许可发送该邮件，且该邮件是作为一个更大邮件集合的一部分进行发送的，所有的邮件内容基本相同。只有当垃圾邮件被用作上述其他 DNS 滥用类型中的任何一种的传递机制时，才会被视为 DNS 滥用。

注册服务机构的义务

RAA 第 3.18 节

在“DNS 滥用修订版”颁布之前，第 3.18 节要求注册服务机构维护并公布详细联系信息以接收滥用报告，其中包括非法活动。这项条款还规定了与调查和响应滥用报告相关的要求，这些滥用报告涉及注册服务机构赞助的注册域名，以及注册服务机构必须维护的相关记录。RAA 第 3.18 节中的要求进行了如下修订：

关于公布和维护滥用行为联系信息的要求 (RAA 3.18.1)

在何处报告滥用行为[3]

为了便于指控滥用行为和/或非法活动的任何一方提交报告，注册服务机构必须在注册服务机构网站[4]的主页上公布便于访问的电子邮件地址或网页表单。使用网页表单提交滥用报告时，不得要求登录。

如果注册服务机构的主页明确显示指向“报告滥用行为”或“联系我们”页面的链接（其中明确包含滥用行为联系信息），并且允许报告者轻松地从链接的页面提交报告，则该主页将被视为合规。

滥用报告的送达确认函

此外，注册服务机构必须向滥用报告者提供已收到报告的确认函。在向注册服务机构提交报告后，该送达确认函会发送给滥用报告者或显示在屏幕上。该送达确认函必须包含足够的信息，以便报告者能够证明其提交了滥用报告。送达确认函必须至少标明注册服务机构、报告的注册域名和提交报告的日期。

执法机构的联系信息

与专门接收法律报告的联系信息相关的要求先前在 RAA 第 3.18.2 节中描述的注册服务机构所在司法管辖区的执法机构 (Law Enforcement Agencies, LEA) 和其他权威机构现在包含在 RAA 第 3.18.3 节中；这些要求保持不变。

与在收到可操作的 DNS 滥用报告后采取缓和措施相关的要求 (RAA 3.18.2)

经“DNS 滥用修订案”修改后，RAA 第 3.18.2 节现在包含如下内容：

> *当注册服务机构具备可操作证据，证明注册服务机构赞助的注册域名被用于实施 DNS 滥用行为时，注册服务机构必须立即采取合理必要的适当缓和措施，以便阻止或 以其他方式中止注册域名被用于实施 DNS 滥用行为。考虑到 DNS 滥用行为所造成损害的原因和严重程度以及相关间接损害的可能性，采取的措施可能会根据具体情况而有所不同。*

[3] 为免存疑特此说明，与通过注册数据目录服务 (Registration Data Directory Service, RDDS) 公布注册服务机构滥用行为联系电子邮件地址和电话号码相关的要求保持不变。

[4] 该网站应位于注册服务机构通过其 RDDS 显示为“注册服务机构 URL”字段值的同一统一资源定位符 (Uniform Resource Locator, URL) 中，并被提供给 ICANN 和注册管理运行机构，以便在注册管理运行机构的 RDDS 中公布。

可操作证据

证据必须具有*可操作性*。这意味着，注册服务机构随时可获得的信息必须足以使注册服务机构合理认定注册域名是否被用于实施一种或多种形式的 DNS 滥用行为。我们鼓励注册服务机构主动监控他们赞助的注册域名，以识别潜在的 DNS 滥用行为。注册服务机构对可操作证据的评估将根据每个案例的情况而有所不同。

从外部方获取可操作证据

签约方机构 (Contracted Parties House, CPH) 公布了相关指南，以协助向注册服务机构提交完整且可操作的滥用报告（CPH 指南）。《CPH 指南》描述了使滥用报告具有可操作性的证据。例如，一张显示网络钓鱼攻击尝试的屏幕截图，其中指明了网络钓鱼的攻击目标（例如金融机构）；以及发生滥用行为的完整 URL（例如 example[.]tld/badpage[.]html）[5]。我们鼓励滥用报告者查看并遵循《CPH 指南》，并在报告中提供尽可能多的信息，以便注册服务机构能够针对潜在 DNS 滥用行为开展调查。

如果注册服务机构收到的滥用报告不包含被视为 DNS 滥用行为可操作证据的所有必要信息，那么注册服务机构必须根据 RAA 第 3.18 节开展调查。在某些情况下，注册服务机构可以获取滥用报告者未提供的信息，但对于确定注册域名是否被用于实施 DNS 滥用行为而言，这些信息是必要或有帮助的。在这种情况下，注册服务机构应考虑其可以合理获取且与调查相关的信息（例如，域名服务器、帐户信息和活动，以及滥用报告中至少包含的主要网页或特定 URL 内容（如果提供））。

在获得可操作证据后，需要立即采取措施

在获得可操作证据后，注册服务机构必须*立即*采取合理必要的*适当缓和措施*，以便阻止或以其他方式中止

[5] 此 URL 以一种称为“判定为无效的 URL”的格式显示。判定为无效的 URL 肉眼可见，但无法点击。因此，如果您或者滥用报告的收件人误点了该 URL，它不会将您或收件人定向到潜在的恶意网站。

注册域名被用于实施 DNS 滥用行为。为了确定及时且适当的缓和措施，注册服务机构将考虑案例的具体情况，其中可能包括权衡 DNS 滥用行为造成损害的范围和强度与可能造成的相关间接损害。

当某个原本合法或良性的域名在注册人不知情或未同意的情况下被用作 DNS 滥用矢量时，间接损害是一个特别重要的考虑因素。这通常称为“受损域名”，有时候是网站内容管理系统漏洞被利用所导致的结果。在这些受损情况下，注册服务机构或注册管理运行机构直接暂停域名可能并不是适当的缓和措施，因为暂停域名将切断对所有合法内容的访问，使任何与该域名相关的电子邮件和其他服务无法访问[6]。当 DNS 滥用与三级域或子域相关时，情况也是如此。注册服务机构和注册管理机构只能在二级域采取措施。因此，如果他们暂停二级域，所有三级域也将被暂停，而不仅仅是与 DNS 滥用相关的域名。在这些情况下，注册服务机构可能会选择向注册人、网站运营商和/或网络托管商提供通知。

采取即时措施的要素

如上所述，阻止或中止 DNS 滥用事件的适当缓和措施将根据具体情况而有所不同。因此，开展调查和采取措施的相应时间也会有所不同，从而无法规定用来将采取的措施视为“即时”的固定时间。注册服务机构而是必须持续关注对赞助域名被用于实施 DNS 滥用行为的指控。这种关注应与 DNS 滥用对受害者造成的潜在损害相称。

因此，在回应 ICANN 合同合规部的问询时，注册服务机构需要说明，考虑到具体情况是如何采取即时措施的。随后，ICANN 合同合规部将审核该说明和相关情况，逐一确定这些措施是否合理即时。本公告中所包含示例的时间表并不是合规要求，而只用于说明目的。注册服务机构花费较长时间对与示例相似的案例开展调查和采取措施时，这并不一定表明存在违规行为。相反，在其他一些情况下，注册服务机构可能需要更快速地采取措施，例如可能对最终用户造成迫在眉睫的损害

[6] 有关间接损害和在 DNS 级别采取措施时的相称性考量的更多信息，请参阅互联网与管辖权政策网络的发布文件“工具包：DNS 级别滥用应对行动方案”。

的 DNS 滥用事件。在注册服务机构合理尝试确认 DNS 滥用事件之后，注册服务机构应尽快开展调查并采取措施。

汇总 – 注册服务机构合规示例

下面的示例说明了为阻止注册域名被用于实施 DNS 滥用行为（情景一）和中止与注册域名相关的 DNS 滥用过程（情景二）而采取的合理且即时的缓和措施。这些情景包含具体的实际情况。在不同情况下，各注册服务机构可能会在不同的时间范围内采取不同的措施来阻止或以其他方式中止个别 DNS 滥用案例。在所有情况下，注册服务机构必须能够证明所采取的任何方法都符合 RAA 第 3.18 节中的相关要求。

情景一：注册服务机构收到一份完整且可操作的滥用报告，指控注册服务机构赞助的注册域名被用于网络钓鱼。这份报告包含的证据表明，不法分子正在通过电子邮件或短信发送一个包含注册服务机构所赞助的注册域名的 URL，并且自称是一家大型银行，要求收件人解锁其账户。注册服务机构根据滥用报告中包含的所有相关信息开展调查。注册服务机构的调查显示，该注册域名没有公开可用的网站，并且仅显示一个直接 URL，这似乎是一家大型银行的登录屏幕。而同一 URL 正在通过电子邮件或短信发送。注册服务机构还将该客户视为新客户，并且注册域名是在五天前注册的。

适当的缓和措施：注册服务机构合理认定注册域名被用于实施 DNS 滥用行为，并通过暂停注册域名，应用 clientHold 可扩展供应协议 (Extensible Provisioning Protocol, EPP) 状态编码[7]来阻止实施 DNS 滥用行为。在收到滥用报告的两个工作日内开展了调查并采取了缓和措施。只要注册服务机构遵守 ICANN 转让政策中的适用要求，注册服务机构还可以决定对注册域名应用转让锁定期，以阻止注册人试图逃避缓和措施并继续使用域名实施 DNS 滥用行为。

情景二：注册服务机构收到一份完整且可操作的滥用报告，指控注册服务机构赞助的注册域名 autobrand.tld 被用于网络钓鱼。滥用报告中包含的证据表明，某个特定 URL 正被用于网络钓鱼。注册服务机构根据滥用报告中包含的所有相关信息以及注册服务机构可轻松且合理获取的信息开展调查。

[7] 点击此处了解 ICANN 提供的有关 EPP 状态编码的更多信息。

调查证实，滥用报告中的 URL 正被用于网络钓鱼。调查还显示，该 URL 属于子域 (city.autobrand.tld)，并且似乎由特许经营商使用。注册服务机构承认，注册域名 autobrand.tld 是在三年前注册的，且包含汽车经销商特许经营的丰富内容。注册服务机构能够确认，该注册域名用于 Autobrand 的公司电子邮件和多家特许经营商的子域。

适当的缓和措施：注册服务机构合理认定，注册域名正被用于实施 DNS 滥用行为，但这很可能导致域名受损，并且注册人并非故意将注册域名用于实施 DNS 滥用行为。注册服务机构评估暂停域名可能造成的潜在间接损害，并合理地得出结论，认为这不是目前适合采取的缓和措施。为此，注册服务机构通知 autobrand.tld 的注册人 Autobrand，要求其在注册服务机构合理确定的某个日期之前删除网络钓鱼内容，从而中止 DNS 滥用行为。在收到滥用报告的三个工作日内开展了调查并采取了缓和措施。

与维护和向 ICANN 提供记录相关的要求

先前在 RAA 第 3.18.3 节中描述的与记录接收并回应滥用报告相关信息和提供该记录相关的要求现已包含在 RAA 第 3.18.4 节中；这些要求保持不变。这些要求也适用于第 3.18.2 节规定的 DNS 滥用报告回应。

注册管理运行机构的义务

RA 规范 6 第 4 节

RA 规范 6 第 4 节要求向 ICANN 公布和提供详细联系信息，以处理与顶级域 (Top-Level Domain, TLD) 中的恶意行为相关的问询。它还包括与在恶意行为有关的情况下删除孤立粘合记录相关的要求。此规范中的要求进行了如下修订：

关于公布和维护滥用行为联系信息的要求（基本 RA 规范 6 第 4.1 节）

在何处报告滥用行为

为了便于指控 TLD 中恶意行为（包括 DNS 滥用）的任何一方提交报告，注册管理运行机构必须公布电子邮件地址或网页表单、邮寄地址和主要联系人，以便处理此类报告。

如果注册管理运行机构的主页明确显示指向“报告滥用行为”或“联系我们”页面的链接（其中明确包含滥用行为联系信息），并且在该页面上提交报告不受阻碍，则该主页将被视为合规。

滥用报告的送达确认函

收到报告时，注册管理运行机构应向滥用报告者提供已收到报告的确认函。在向注册管理运行机构提交报告后，该送达确认函会发送给滥用报告者或显示在屏幕上。该送达确认函必须包含足够的信息，以便报告者能够证明其提交了滥用报告。送达确认函必须至少标明注册管理运行机构、报告的注册域名和提交报告的日期。

与在收到可操作的 DNS 滥用报告后采取缓和措施相关的要求（基本 RA 规范 6 第 4.2 节）

经“DNS 滥用修订案”修改后，规范 6 第 4.2 节现在包含如下内容：

> *如果注册管理运行机构根据可操作证据合理认定该 TLD 的注册域名被用于实施 DNS 滥用行为，则注册管理运行机构必须立即采取合理必要的适当缓和措施，以便有助于阻止或以其他方式中止域名被用于实施 DNS 滥用行为。此类措施应至少包括：(i) 将正被用于实施 DNS 滥用行为的域以及相关证据转交给赞助注册服务机构；或 (ii) 注册管理运行机构在认为合适时采取直接措施。考虑到 DNS 滥用行为所造成损害的严重程度以及相关间接损害的可能性，采取的措施可能会根据各个案例的具体情况而有所不同。*

可操作证据

证据必须具有*可操作性*。这意味着，注册管理运行机构随时可获得的信息必须足以使注册管理运行机构合理认定注册域名是否被用于实施一种或多种形式的 DNS 滥用行为。注册管理运行机构可以通过审核其能够合理独立访问的信息来获取可操作证据，这些证据可与滥用报告结合使用，也可以在根据《注册管理机构协议》规范 11(3)(b) 而开展的工作中，通过对这些证据进行技术分析来识别被用于实施 DNS 滥用行为的域名。可操作证据也可由外部方提交给注册管理运行机构，例如 LEA、注册管理运行机构信任或认可的相关来源，或者任何其他方或来源。我们鼓励滥用报告者提供尽可能多的信息，以确保注册管理运行机构拥有充足的信息就潜在 DNS 滥用行为开展调查。为免存疑特此说明，如果注册管理运行机构能够获得充足的信息来合理开展调查，以确定所报告的注册域名是否被用于实施 DNS 滥用行为，则注册管理运行机构认为不完整的滥用报告可能会被视为具有可操作性。

在获得可操作证据后，需要立即采取措施

在获得可操作证据后，注册管理运行机构必须立即采取合理必要的适当缓和措施，以便阻止或以其他方式中止域名被用于实施 DNS 滥用行为。为了确定适当的措施，注册管理运行机构将考虑案例的具体情况，其中可能包括权衡 DNS 滥用行为所造成的损害和受害范围与可能造成的相关间接损害。上述域名受损情况下的间接损害对注册服务机构的重要性同样适用于注册管理机构。

注册管理运行机构还将考虑其自身、赞助注册服务机构和/或其他方是否为最有资格开展审核并采取适当且相称缓和措施的一方。例如，对于正被用于实施 DNS 滥用行为的单个注册域名，注册服务机构可能最适合与其客户一起审核并解决 DNS 滥用问题。同样，在系统受损的情况下，注册域名持有人或对受影响系统具有管理访问权限的托管提供商也许更有能力解决这些问题，注册管理运行机构应首先将这些问题转交给注册服务机构，因为通过应用 clientHold 或 serverHold 来暂停域名可能会对良性或合法的内容造成间接损害。另一方面，注册管理运行机构可能是最适合解决跨多个注册域名持有人或注册服务机构的大规模威胁的一方，例如用来传播僵尸网络的域名生成算法。

采取的即时缓和措施必须合理且必要，以实现以下结果之一：*帮助阻止*或*中止*注册域名被用于实施 DNS 滥用行为。注册管理运行机构必须至少：

1) *报告*注册域名并向赞助注册服务机构*提供*相关证据；或
2) 在注册管理运行机构认为适当的情况下对注册域名*采取直接措施*。

采取即时措施的要素

如上所述，对于注册服务机构，为阻止或中止 DNS 滥用事件而采取的适当措施将根据具体情况而有所不同。

因此，开展调查和采取适当措施的相应时间也会有所不同，从而无法规定用来将采取的措施视为“即时”的固定时间。注册管理运行机构而是必须持续关注对赞助域名被用于实施 DNS 滥用行为的指控。这种关注应与 DNS 滥用对受害者造成的潜在损害相称。

因此，在回应 ICANN 合同合规部的问询时，注册管理运行机构需要说明，考虑到具体情况是如何采取即时措施的。随后，ICANN 合同合规部将审核该说明和相关情况，逐一确定这些措施是否即时。本公告中所包含示例的时间表并不是合规要求，而只用于说明目的。注册管理运行机构在某个特定案例上花费的时间较长并不一定表明存在违规行为。相反，在其他一些情况下，注册管理运行机构可能需要更快速地采取措施，例如可能对大量最终用户造成迫在眉睫的损害的大规模威胁事件。在注册管理运行机构合理尝试确认 DNS 滥用事件之后，注册管理运行机构应尽快开展调查并采取措施。

下面的示例说明了为帮助阻止注册域名被用于实施 DNS 滥用行为（情景二）和帮助中止与注册域名相关的 DNS 滥用过程（情景一和三）而采取的合理且即时的缓和措施。这些情景包含具体的实际情况。在不同情况下，各注册管理运行机构可能会在不同的时间范围内采取不同的措施来帮助阻止或以其他方式中止个别 DNS 滥用案例。在所有情况下，注册管理运行机构必须能够证明所采取的任何方法都符合 RA 规范 6 第 4.2 节中的相关要求。

RA 规范 11 第 3(b) 节

本节已进行修改，使用修订案中所述的定义术语“DNS 滥用”替代了规范 6 第 4 节中的“安全威胁”。

汇总 – 注册管理运行机构合规示例

情景一：注册管理运行机构通过其滥用网页表单收到一家信用合作社 (Example Credit Union) 的通知，称有人在六天前注册了域名 <loginexamplecreditunion[.]TLD>，并且这家信用合作社指控该域名被用于实施网络钓鱼。这家信用合作社提供了一张屏幕截图，其中显示该域名上的某个网页正在收集登录凭证。

适当的缓和措施：按照内部流程，注册管理运行机构会在两个工作日内对报告进行处理和审核。在结束其调查之后，注册管理运行机构合理认定注册域名曾被用于实施 DNS 滥用行为。因此，注册管理运行机构通知赞助注册服务机构并向其提供所有相关信息，以中止 DNS 滥用过程。注册管理运行机构向注册服务机构发出有时限的请求，要求其开展调查并采取合理必要的缓和措施来阻止或以其他方式中止 DNS 滥用行为。在给定的截止日期之前，注册管理运行机构能够通过应用 clientHold EPP 状态编码来确认注册服务机构已暂停注册域名。

情景二：LEA 与注册管理运行机构联系，并提供证据表明有一系列域名正在或将会牵涉到与僵尸网络相关的域名生成算法。该僵尸网络涉及一些现有注册域名，但主要是尚未注册的域名。

适当的缓和措施：在结束调查并合理确认存在 DNS 滥用行为后的六个小时内，注册管理运行机构按照 LEA 指示或与 LEA 商定的方式采取措施，从而帮助阻止 DNS 滥用行为。在这种情况下，注册管理运行机构同意，对于相关注册域名，注册管理机构将根据 LEA 的请求授权给不同的域名服务器（例如重定向域名服务器或转为 DNS 天坑）。注册管理运行机构还将按照 LEA 的请求，直接为那些之前与僵尸网络关联的未注册域名创建域名。请注意，注册管理运行机构创建域名通常需要通过 ICANN 安全响应弃权书 (Security Response Waiver, SRW) [8]获得许可。注册管理运行机构还将及时提出请求以获取合同弃权书。但值得注意的是，也可以在事后合理可行的情况下 -

[8] 有关安全响应弃权书的信息，请参阅此页面。

尽快申请 SRW，并且 ICANN 组织可以在适当时以可追溯的弃权书作为回应，以免延误对 LEA 运营的支持[9]。

情景三：在根据规范 11(3)(b) 开展技术分析以查找 DNS 滥用行为的过程中，注册管理运行机构发现某个域名的子页面正被用来分发恶意软件，而该域名上网站的其余页面似乎为合法或良性内容。该域名已注册三年。

适当的缓和措施：在确定注册域名正被用于实施 DNS 滥用行为并受到损害后的三个小时内，注册管理运行机构通知赞助注册服务机构并向其提供所有相关信息，同时要求注册服务机构在规定时间内采取措施并向注册管理运行机构汇报，从而帮助中止 DNS 滥用过程。随后，注册服务机构直接通知注册人，注册人通过更新其内容管理系统以移除恶意软件来解决问题。

ICANN 组织针对是否遵守 RAA 新的第 3.18.2 节和 RA 规范 6 第 4.2 节开展的调查

构成完整、证据充分且合规回应的要素是什么？ICANN 合同合规部将通过处理外部投诉、主动监控和审计活动来强制执行本公告中阐述的要求。当 ICANN 合同合规部收到投诉时，该部门将审核报告者提交的所有证据以及任何可用的相关信息，以确定是否必须向相关注册服务机构或注册管理运行机构发起合规案例。如果没有充足证据支持对 DNS 滥用的控诉，ICANN 合同合规部会将案例视为无效并结案。除其他事项之外，此审核还将考虑直接或通过分销商或注册管理运行机构（如果适用）向赞助注册服务机构提供的现成信息是否足以合理认定注册域名正被用于实施一种或多种形式的 DNS 滥用行为。另外，此审核也将考虑报告方是否根据

[9] 有关注册管理机构如何与执法机构和 ICANN 合作解决域名生成算法的更多信息，请参阅政府咨询委员会公共安全工作组和 gTLD 注册管理机构利益相关方团体发布的“与恶意软件和僵尸网络相关的域名生成算法框架”。

注册服务机构或注册管理运行机构关于提供补充信息或证据的请求提供了任何补充信息。

此外，在适用并与具体案例相关的情况下，ICANN 合同合规部将：(1) 审核通过注册数据目录服务显示的公众可访问的相关数据，例如创建日期、EPP 状态或域名服务器信息；以及 (2) 执行 DNS 查找以确定所报告的注册域名是否在 DNS 中解析。ICANN 合同合规部也可以自行开展研究，并就被指控为参与 DNS 滥用行为的特定注册域名审核相关补充信息。

当分别根据 RAA 第 3.18.2 节或 RA 规范 6 第 4.2 节向注册服务机构或注册管理运行机构发起
合规案例时，ICANN 合同合规部将提供一份逐项列举的清单，其中包含评估合规性所需的所有信息和记录，因为它与报告的注册域名和涉嫌 DNS 滥用的形式有关。为了回应合规案例，注册服务机构和注册管理运行机构至少应当：

- 如果适用，说明注册服务机构或注册管理运行机构如何以及为何确定所获得的证据不具有可操作性。例如，注册服务机构可能会说明，在审核报告方提交的信息和记录并且经过调查后，注册服务机构无法验证 DNS 滥用行为是否与所报告的注册域名有关。当所提供的说明与 ICANN 合同合规部在合规性验证流程中捕获的任何信息和数据之间存在任何明显差异时，ICANN 合同合规部可能会要求注册服务机构或注册管理运行机构对此进行澄清。
- 提供详细说明并附有相关记录，说明所采取的具体缓和措施，采取这些措施的时间，以及对于阻止或中止（或者帮助阻止或中止）滥用行为，所采取的措施是如何被认为是即时且合理必要的，因为这与案例的具体情况有关（其中包括与 DNS 级别所采取措施的不相称性和间接损害有关的任何适用解释）。如果注册服务机构选择将 DNS 滥用报告的调查授权给分销商，则对注册服务机构提供此信息的要求将继续适用。在这种情况下，注册服务机构仍有义务通过解释其采取的措施以及分销商等任何其他授权方采取的措施，并提供相关记录，来证明其遵守 RAA[10] 第 3.18 节的规定。

[10] 请参阅 RAA 第 3.12 节。

ICANN 政策和合规要求在适用于各注册服务机构和注册管理运行机构的法律和法规范围内实施。为免存疑特此说明，注册服务机构和注册管理运行机构均无需或不应采取任何违反适用法律和法规的措施。

有关何时、如何以及在何处向 ICANN 合同合规部提交投诉的信息，可在此处获取。