ICANN78 | 筹备周 — 域名冲突分析项目研究 2 最新资讯
2023 年 10 月 10 日星期二 — 汉堡时间 10:00 至 11:00

凯西 • 什尼特
(KATHY SCHNITT)： 大家好，欢迎参加域名冲突分析项目研究 2 最新资讯会议。我叫凯西，是本次会议的远程参会经理。

请注意，本次会议正在录制中，请大家遵循 ICANN 预期行为标准。会议期间，在问答窗格提交的问题或意见将在预留的问答时间被读出来。聊天窗口中的问题不会被读出来。

本次会议的口译将包括英语、法语、西班牙语、中文、俄语、阿拉伯语和葡萄牙语。大家可以点击 Zoom 中的“同声传译”图标，选择在会议期间要收听什么语言。

如果你想发言，请在 Zoom 会议室中举手示意，在会议主持人叫到名字后，请将你的麦克风取消静音并发言。请说出你的姓名以便记录，如果你使用的不是英语，也请指明你将使用的语言。发言时，请确保将所有其他设备和通知静音。请大家发言时口齿清晰并保持正常语速，以便口译人员能准确翻译。

本次会议包括自动实时速记。请注意，速记文稿并非官方会议记录，也不具有权威性。若要查看实时速记，请点击 Zoom 工具栏中的“隐藏字幕”(Closed Caption) 按钮。

为确保 ICANN 多利益相关方模型的参与透明度，我们要求你在 Zoom 会议中使用全名签到。

我就先说到这里，现在很高兴交给 NCAP 联合主席马修 • 托马斯 (Matthew Thomas)。

马修 • 托马斯： 谢谢凯西。我是马修 • 托马斯，NCAP（域名冲突分析项目）联合主席之一，另一位联合主席苏珊 • 沃尔夫 (Suzanne Wolf) 也在这里。我们很高兴今晚或者说是今天能在这里向大家介绍域名冲突分析项目的最新情况。

我们希望本次会议能让大家了解域名冲突项目在过去几年中的发展动向，以及我们目前的现状，并希望会议保持简短。请翻到下一页。

今天我们将简略介绍一下域名冲突的背景。凯西在介绍时说过，这是域名冲突的研究 2。我们想略微介绍一下研究 1 的背景，以及我们在研究 2 中正在做的工作。接下来，我们将讨论研究 2 中已完成的一些工作，特别是一些已完成的研究和报告。

接下来，我们将讨论 ICANN 董事会正式要求讨论小组和 SSAC 提供建议和指导的董事会问题；然后讨论我们目前的研究结果，这将有助于讨论以可持续和可重复的方式解决域名冲突问题的潜在工作流程；最后，我们将介绍如何参与 NCAP 的一般信息，并留出问答时间。请翻到下一页。

我想介绍一下背景情况。这张幻灯片将纳入即将发布的“研究 2”报告中，描绘了过去 10 多年中与域名冲突有关的历史性重要里程碑。显然，从这张图或图表中可以看出，围绕域名冲突的研究分析、指导和防护措施已经做了大量的工作。

我认为，每个人都必须真正了解域名冲突的所有历史背景，才能真正充分理解研究 2 的发展方向和尝试实现的目标。

显然，我们无法一一列举和讨论所有这些重要的里程碑，但当你们有机会阅读研究 2 报告时，我们会在详细介绍域名冲突的背景和历史时，讨论该图表上的这些带注释的数字或标注，希望这能为如何评估域名冲突以及 NCAP 讨论小组提出的未来风险管理解决方案提供足够的背景和见解。请翻到下一页。

具体而言，域名冲突分析项目是 ICANN 董事会向 SSAC 提出要求后产生的，董事会要求 SSAC 开展一些研究，以提供数据分析和有根据的观点，并就一般域名冲突问题向董事会提出建议。其中有一个是针对 .home、.corp 和 .mail 字符串提供建议的请求，以及一系列针对未来名称冲突的更一般性建议的问题。

NCAP 讨论项目或小组已经开展了数年。我认为我们已经进入第四年或第五年了。我们一直在以全面和包容的方式开展工作，纳入社群内的技术和非技术专家。大约有 25 名讨论小组成员积极参与，其中 14 名是 SSAC 工作组成员。我们还有大约 23 名社群观察员。请翻到下一页。

与 NCAP 相关的信息相当多。由于信息量非常大，我们无法在此详述，但当这些幻灯片公开后，我们将向大家推荐有关这四个主要项目的链接，在这些链接中，大家可以看到向 SSAC 提出以及随后向 NCAP 讨论小组提出的确切的董事会决议或问题，以及项目章程和项目建议书。

最重要的可能是社群维基主页，其中包括 NCAP 讨论小组最近 100 次电话会议的录音、演示文稿、报告等，在这里可以看到这个项目中开展的所有工作。请翻到下一页。

总的来说，NCAP 研究实际上分为三个不同的阶段。研究 1 是围绕域名冲突进行差距分析。这项研究有两大目标，首先是给出域名冲突的正确定义。

如果你还记得，在我们展示的第一张历史时间线幻灯片上，你会发现其中一点，那就是域名冲突的定义在过去十年中发生了变化。域名冲突的内涵和外延并不总是一致的。因此，研究 1 的主要目标之一就是提出域名冲突的正确定义。

第二个主要目标是对以往所有研究中的域名冲突问题进行详尽研究，并对域名冲突方面的工作和研究进行潜在的差距分析。

现在，研究 1 的工作已于几年前完成。报告已征求公众意见，并已正式发布。但是，作为这项工作的成果，结合 NCAP 讨论小组的工作，发现确实存在一些差距，特别是在 DNS 的技术和演进方面，以及 DNS 生态系统自 2012 年至今是如何演进的，由此产生了修改和修订后的研究 2 提案。

研究 2 是 NCAP 讨论小组目前的工作，修订后的目标和目的如下。之前的目标和目的较大，即尝试创建数据存储库和一些被认为无法进一步实现的东西。

但目前的工作重点是确定构成冲突字符串的标准，以及如果某个字符串被认为是冲突字符串，确定允许将其从冲突字符串列表中删除的标准。它还要求对域名冲突的各种相关因素进行一些具体研究，稍后将在这里进行 [听不清] 讨论。

现在，尚未进行的最后一项研究是研究 3，即对缓解方案的分析。我要指出的是，就在早些时候，也就是上周，NCAP 讨论小组举行了一次为期两天的研讨会，许多成员参加了这次研讨会，并花了整天的时间来讨论各种域名冲突的问题。

这次研讨会的重要收获之一是，讨论小组根据其目前的理解/发现，以及研究 3 中提议的范围和职责，并考虑到我们对缓解方案的了解，很可能建议不进行研究 3。

简而言之，缓解方案很可能会按具体字符串或具体域名冲突进行量身定制。实际上，并不存在通用的域名冲突补救或缓解策略，小组认为，这可以反映在我们的研究 2 说明中；研究 3 目前可能没有必要开展。请翻到下一页。

那么，研究 2 的进展如何？我之前提到过，除了研究 2 中的这些高层次目标外，还要求开展三项具体研究。第一项研究是关于字符串冲突的案例研究。我们之前提到过，董事会的一项决议特别要求就 .corp、.home 和 .mail 提供建议。这就是案例研究的目的所在。

不过，我们并没有只研究 .corp、.home 和 .mail，而是在研究中增加了 .internal、.lan 和 .local 这三个字符串，原因很简单，因为在研究期间，这三个字符串在 A 和 J 根服务器上的日查询量也超过了 1 亿次。

该案例研究的目的是了解工作重点和随时间推移发生的变化。这是对在 A 和 J 根服务器观察到的 DNS 流量进行的一项纵向研究，时间大致可追溯到 2015 年，研究内容是 DNS 流量因这六个不同字符串的域名冲突发生了什么变化或者改变。

第二项研究是针对不存在的顶级域的 DNS 查询的视角研究。这项研究的真正目的是尝试更好地了解 DNS 遥测数据可以在 DNS 层次结构中的不同有利位置（特别是根服务器系统以及递归解析器）使用的位置、方式和可信度，以了解 DNS 域名冲突流量。

其目标实际上是提供一些见解，即如何以及在何处收集和评估 DNS 数据，以及在今后用于评估域名冲突及其潜在风险时，需要为这类数据设置哪些适当的防护措施。

最后一项研究是根本原因分析。这项研究是由 ICANN 的一名签约技术调查员进行的，他利用了 ICANN 自 2012 年以来收到的 40 多份域名冲突报告，这些报告涉及通知机制产生的各种域名冲突问题，并且可能与控制性中断问题有关，并了解了这些事件是如何报告的、域名冲突对这些当事方产生了哪些影响，同时还将这些域名冲突与任何类型的 DNS 遥测数据关联起来，以确认或否认相关域名冲突的识别支持。请翻到下一页。

这三项研究都已经开展了。前两项研究已经征求公众意见。第三项研究已经最终完成。至少在 NCAP 讨论小组内部已达成共识。这三项研究得出了一些关键结论。

第一个是，再次关注 .corp、.home 和 .mail。研究清楚地表明，这些字符串的潜在影响逐年增加，特别是在过去几年的疫情期间。

关键诊断测量是一种量化测量方法，NCAP 讨论小组帮助构建并形成了这种方法，同时还结合了 [听不清] 等人和 JAS 先前研究的出色工作及其评估结果，其中域名冲突可通过 DNS 的不同指标（如 DNS 查询值）进行量化，但也包括其他维度（如多样性），其中多样性可跨越多个不同矢量，如名称多样性、QTYPE 多样性、网络多样性等。

案例研究还发现，DNS 服务发现协议和后缀搜索列表仍然是整体上导致域名冲突的一些主要问题。WPAD（网络代理自动发现）或 ISATAP（IPv6 隧道服务）等都是造成问题的主要因素。

与此同时，第二项研究是 DNS 查询视角研究，该研究探讨了如何以及在何处评估 DNS 流量，深入分析了每个根服务器身份的异同，以及根服务器与大型公共递归解析器之间的差异。

这些分析有助于形成未来的一些潜在机会，或许可以加强或扩展新的测量平台，以便在潜在申请人提交申请之前为其提供更多的域名冲突 DNS 遥测数据。这些系统，例如 ICANN 的 ITHI 或 ICANN 的 IMRS 系统，已经可以对潜在的域名冲突风险进行一些分析。

最后，我们还进行了根本原因分析，对这 40 多份报告进行了研究。该报告再次表明，私人使用 DNS 后缀的情况仍然非常普遍；域名冲突报告是通过从被动 DNS 数据源收集的数据进行有力衡量的；最重要的是，在之前的 2012 轮次，向 ICANN 提交的域名冲突报告中，TLD 授权的影响从无影响到严重影响不等。

在域名冲突问题上，我认为我们从所有这些重要结论中看到的是，域名冲突现在是、将来也仍将是一个难以识别和补救的问题。请翻到下一页。

珍妮弗 • 布莱斯 (JENNIFER BRYCE)： 马修，由于演讲具有技术性，口译员问你能不能稍微讲慢一点。

马修 • 托马斯： 好的。我会尽力而为。谢谢，珍妮弗。好的。希望这不是技术性的讨论。但最初董事会决议的主要任务之一是回答董事会提出的几个问题并提供建议和/或指导。董事会的这些问题实际上包括九个不同的问题，其中第一个问题是正确定义域名冲突。这已经最终确定，并在研究 1 中征求公众意见。大家可以在 ICANN 资源中看到这一点。

其余七个问题没有在此明确概述，而是被纳入主题的粗略分类中，范围涉及一组主题，例如考察否定应答的作用。目前，域名冲突字符串期望从域名系统 (DNS) 的根服务器得到否定应答。

因此，了解这些否定应答会如何影响潜在的终端系统、用户或申请非常重要。随后，问题三的重点是：如果不再返回这些否定应答，可能会造成什么潜在危害，这些申请和系统中的哪些方面可以改变，以及当不再返回否定应答时，可能会造成什么潜在危害？

接下来，问题四和五探讨了减轻这种危害的潜在方法。是否有技术/工具/程序可用于帮助防止与域名冲突有关的危害？

问题六：实际授权域有哪些风险？最后是问题七、八和九。这些都与未授权字符串、冲突字符串以及这些字符串的一般管理有关。

NCAP 讨论小组已经就董事会问题提供了这些回答和建议的初稿。NCAP 讨论小组内部已达成粗略共识。

不过，由于我们将在下一部分讨论工作流程，小组希望在研究 2 报告接近最终完成时更新这些问题，以便董事会问题的建议和回答能够与研究 2 报告中的大量工作材料、结论和建议更加紧密地相互参照。请翻到下一页。

说到研究结论，我们目前有一套粗略的结论，你们可以在这里看到。正如我之前所说，我们已经对域名冲突的实际含义以及与 ICANN 社群相关的某些情况下的域名冲突做出了适当的最终定义。

我们还确定，域名冲突现在是、将来也仍然是一个越来越难以识别和补救的问题。我们的案例研究也证明了这一点，因为我们看到影响已经扩大。我们可以从 DNS 服务发现协议的激增和后缀搜索列表的增长中看到这一点。但我们也 [注意到]，未来仍有可能发生不良冲突。

我之前提到，我们还围绕关键诊断测量 (CDM)，对域名冲突的识别和量化达成了共识。这些方法有助于定量描述与 DNS 流量相关的潜在遥测数据，从而了解域名冲突的潜在风险或影响。不过，小组也会注意到，域名冲突仍有定性的成分，需要对所有字符串进行评估。

此外，这还与数据的局限性有关，并且 DNS 内部对于评估域名冲突的能力仍然存在局限性，而且局限性越来越大，就像 2012 年轮次那样。

如前所述，修订研究 2 的主要驱动力之一是技术差距分析，讨论小组发现 DNS 生态系统中的重大变化已经损害或严重降低了域名冲突的可见性，原因是限定名称最小化、积极的 NSEC 缓存、引入公共递归解析器等技术变化。

小组还发现，至少在下一轮次之前，创建一个不适用的字符串列表是不切实际的。尽管如此，如前所述，我们发现现有的测量平台仍有潜在的扩展机会，可以帮助申请人在提交申请时事先了解潜在的域名冲突风险。这类信息很可能会反映在某些类型的定量 CDM 类型的测量中。请翻到下一页。

工作流程。我们之前提到，董事会正式指示 SSAC 和 NCAP 讨论小组回答这一系列问题，并围绕域名冲突提供建议。然而，真正需要的是建立某种可持续、可重复和可确定的模型，以便能够评估域名冲突的影响和未来的风险。这种方法或工作流程实际上是为了帮助识别那些不应授权的高风险标签。

除了这些高风险标签外，基本假设是所有其他字符串都将通过后续程序中的典型采购和引入流程进行。因此，域名冲突分析项目的真正框架是将其作为一个风险管理问题。

如何在风险管理框架内评估域名冲突？我们如何客观地识别和区分高风险标签与事实上应正常处理的标签？能不能提前识别某些字符串？请翻到下一页。

因此，为了进行评估，需要做的事情之一就是提供数据，以评估域名冲突的潜在风险或影响。这可能意味着可以采用多种不同的测量方法或技术，以便提供数据，在风险管理问题的背景下做出明智的决策，正如我们之前所讨论的那样。

此外，工作流程的目标还包括在需要时，为高风险字符串提供制定潜在缓解或补救计划的机会。正如我们前面所说，讨论小组的目的是提出建议，即不应继续进行围绕缓解计划的研究 3。

这一建议源于这里所说的很多内容，即根据讨论小组过去几年的研究和观察结果，补救和缓解计划似乎是一次针对一个冲突专门制定的。笼统的、一刀切的解决方案似乎并不是解决域名冲突问题的理想的或可实现的解决方案。请翻到下一页。

这大致就是 NCAP 讨论小组多年来一直在研究的潜在的拟议工作流程和时间表。这实际上是一个分为五步的流程，而这五步是以一种合乎逻辑、规避风险的方式进行或设计的。

这里的风险规避是指在不干扰 DNS 生态系统的情况下，首先对最易获取的数据进行域名冲突评估，然后再进行下一步，在下一步中，可以通过技术或操作变更来收集更多的域名冲突数据，并做出明智的评估。

如果我们浏览一下最左侧的工作流程，就会发现申请人可能正在进行静态评估。这其实是申请人在提交申请之前，可以访问 ICANN 的 ITHI 或 IMRS 系统等发布域名冲突相关数据的资源，进行简单的分析，看看他们的字符串是否已经包含在这些已发布的域名冲突数据中。

该字符串是否被纳入这些列表并不意味着最终确定它是好是坏，但它至少是一个先行指标，能让申请人在提交申请前做出一些明智的决定。关于第一点，这被认为是一个潜在的匝道机会。目前，讨论小组仍在讨论匝道如何安装的问题。

但是，在这一工作流程中，匝道的总体目标的设计和概念是为申请人和 ICANN 提供能够退出这一工作流程的能力，而不是在十年后陷入拥有 .corp、.home 和 .mail 等字符串的炼狱状态。希望这将使执行期更加确定且有限。

因此，一旦提交了申请，就会进入申请处理程序。这将与后续程序中的其他流程混合在一起。域名冲突评估发生的时间并没有准确确定，但根据尝试向 ICANN 提供的一般建议、防范措施和指导方针，这在某种程度上是无关紧要的。

但下一个主要步骤将进入技术审核小组，或称 TRT 静态评估。该技术审核小组是一个实体 — 第三方、中立方 — 在评估 DNS 流量数据、了解域名冲突问题、根据他们能收集到的数据评估数据和字符串的潜在影响或风险方面具有专长。

TRT 正在为授予 TLD 的流程提供意见。但在静态评估过程中，TRT 也只是查看在提交申请之前提到的来源，如 ITHI 或 IMRS，或 TRT 可能有权限访问的任何其他数据。

如果没有发现异常或严重风险，评估流程将进入下一阶段，即被动冲突评估 (PCA)。

这是一个正在提议的新阶段，其中所申请的 TLD 实际上被授权到根区，授权指向权威的顶级域名服务器，这些服务器为具有特殊记录类型的通配符区提供服务，该通配符区将以“无空间和无数据”进行响应，但实际上与存根解析器之前收到的 NXDOMAIN 响应等效。

这种授权和数据收集的作用 — 或者说这种授权的作用 — 是与依赖某些静态数据源（如单一根字母实例或来自根的 DNS 数据的其他快照）相比，它提供了更强大、更广泛的数据收集。

这实际上允许在整个根服务器系统范围内进行收集，有助于绕过我们之前提到的一些技术变化，如限定名称最小化、积极 NSEC 缓存等，以提供更丰富的数据，让 TRT 作出更明智的决定。

在“被动冲突评估”之后，下一阶段将进入“主动冲突评估”阶段。主动冲突评估仍在讨论小组内进行讨论。目前正在讨论一套工具和技术，讨论每种工具和技术的作用和使用方法。

但究其核心，这些工具和技术的目的都是为了实现两大目标。其一，收集额外数据，其中大部分数据最终会成为实际受影响设备的数据，因为收集的是它们的 IP 地址，而不是递归解析器。其次，尝试向那些遭受域名冲突问题的受影响实体提供某种通知机制。

一旦“主动冲突评估”阶段结束，技术审核小组将完成其分析，并将其“通过/不通过”评估结果纳入一般流程，以促进新 [TLT] 的其余引入工作，完成在 ICANN 流程内的最终授予程序。

这也是一个简要的概述。在这方面已经达成了粗略的工作共识。有些细节仍在讨论小组内讨论。这是关于希望未来向 ICANN 提出的可持续、可重复模型的总体工作共识。请翻到下一页。

这也是关于技术审核小组的一点介绍。这里谈的是他们的一些角色和责任。在这里，我们只是简单地说，他们必须是独立、中立的专家。他们必须具备 DNS 专业知识、域名冲突专业知识，还能将所有这些知识纳入风险评估框架。他们负有下面列出的四项责任。请翻到下一页。

那么如何参与呢？但愿 NCAP 即将完成研究 2 报告。我们的目标是在年底前就研究 2 征求公众意见。但我们一直在寻找新成员、新声音和新想法。这里有加入讨论小组的链接。我们欢迎大家前来参加。

如果没有，请注意，希望研究 2 报告很快就会发布，征求公众意见，我们鼓励你们阅读该报告。报告会很长、很详细，并且具有技术性。但希望它也能简明扼要地表达在域名冲突方面需要表达的观点，以及如何将其纳入 ICANN 的全局。请翻到下一页。

我就讲到这里，我想问问我的联合主席苏珊，我有没有漏了什么，或者她是否想补充其他内容或评论。如果没有，我们就进入问答环节。

苏珊 • 沃尔夫： 你讲得很透彻。我没有记下任何需要补充的内容，所以我很乐意听大家提问。

凯西 • 什尼特： 好的，马修和苏珊，目前我们没有任何问题。

苏珊 • 沃尔夫： 看，你把要讲的都讲了，马修。

马修 • 托马斯： 非常好。希望这是我们就此进行的最后一次最新资讯通报，下一次通报将是关于实际发布的报告。对吧？

苏珊 • 沃尔夫： 还有公众意见和一些好消息。

马修 • 托马斯： 没错。

凯西 • 什尼特： 实际上，有人举手了。塞巴斯蒂安 (Sebastian)，你可以提问了。

萨巴斯蒂安 • 杜克斯 (SEBASTIEN DUCOS)： 大家好。我是来自 GNSO 的萨巴斯蒂安 • 杜克斯。我们能往前翻两页，回到有关时间表的那张幻灯片吗？可能还要再往前一点，抱歉。对，还有一页。就是这个。

在上一轮次，我们推出了著名的控制性中断。如果我没记错的话，在授权后，TLD 必须在 90 天内处于控制性中断状态，在此期间，TLD 实际上不能使用，因为所有流量都被中断了。之后，TLD 就可以使用了。

但在这一时期，TLD 被授权，从注册管理运行机构的角度看，产生了后端运营商成本 — 在某些情况下，这是经过重新协商的，[但无论如何] 都属于 ICANN 成本。

你们现在是否建议，在类似的条件下，这段时间基本上是六个月？或者说，这是已在小组内部讨论过的事情，还是要与 IRT 或其他机构讨论的事情？

苏珊 • 沃尔夫： 你好。实际上，这是目前仍在积极讨论的领域之一：如何缩短我们讨论这一时间表的时间。

有什么要补充的吗 —

萨巴斯蒂安 • 杜克斯： 没有。

苏珊 • 沃尔夫： — 马修？

萨巴斯蒂安 • 杜克斯： 我一定会找到链接，看看到时候能不能参与讨论。谢谢。

凯西 • 什尼特： 没有其他问题了 —

苏珊 • 沃尔夫： 好的。有很多活动部件，所以我们要确保它们相互配合而不会相互冲突。

凯西，请讲。

凯西 • 什尼特： 苏珊，我只是想说没有其他问题了。

马修 • 托马斯： 非常好。好的，如果我们结束了，能把 12 分钟还给大家吗？

凯西 • 什尼特： 太棒了。谢谢。今天的会议到此结束，可以停止录音了。

[会议记录结束]