ICANN72 | 筹备周 — 介绍域名系统安全协调计划技术研究组 (DSFI-TSG)
太平洋夏令时 2021 年 10 月 14 日星期四 — 13:00 至 14:00

温迪 • 普若菲特

(WENDY PROFIT)：

我们现在召开的会议是介绍 DNS 安全协调计划技术研究组。我是温迪 • 普若菲特，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。在本次会议期间，只有在问答框内提交的问题或评论才会被读出。我们会在本次会议的主席或主持人指定的时间读出这些问题和意见。

本次会议提供所有五种联合国语言的同声传译服务。点击 Zoom 中的同声传译图标，并选择你要在本次会议中聆听的语言。

如果你需要发言，请在 Zoom 会议室中举手。对讨论组成员而言，轮到你发言时，主持人会叫你的名字。如果你要以除英语之外的其他语言发言，请在发言之前从同声传译菜单中选择你要讲的语言。另外，请自报姓名并说明你要讲的语言。发言时，请确保将所有其他设备和通知静音。同时，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。

如果你想通过聊天室交流，请使用聊天窗口中的下拉菜单，然后选择回复所有讨论组成员和与会者。这样，每个人都能看到你的评论。请注意，在 Zoom 网络研讨会形式下，私聊只能在讨论组成员之间进行。讨论组成员或标准与会者向其他标准与会者发送的任何消息都会被会议主持人、联合主持人和其他讨论组成员看到。

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。下面，我将把时间交给约翰 • 克莱恩 (John Crain)。

约翰 • 克莱恩： 非常感谢你，温迪 (Wendy)。大家上午好，下午好，晚上好。首先，我要代马跃然 (Göran Marby) 向大家致歉，他希望能在今天的会议上发言，但是很遗憾，他有其他事要忙，所以让我代表他说几句。我是约翰 • 克雷恩，是 ICANN 首席安全、稳定和弹性执行官，也是临时首席技术官，并且一直积极参与这项计划。众所周知，标识符系统的安全、稳定与弹性是 ICANN 使命的核心，是我们的章程和一切事务的重点和中心。

大约两年前，在经历了一系列攻击之后，跃然 (Göran) 和我探讨了我的职责，他问我，我们应该如何帮助 ICANN 更好地促进标识符系统的安全性。我们提出的流程是，建立一个由来自 ICANN 社群内部以及社群之外来自安全领域的专家组成的技术研究组。本周早些时候，跃然收到了技术研究组提供的一份报告，我们打算下周初将它和跃然的一篇短期博客一并发布到 ICANN 网站上。我想代表跃然对这个小组的辛勤工作表示感谢。一年多以来，志愿者们一直致力于制定这一系列建议。我也参与了其中的工作，所以我知道志愿者们的工作非常努力，我们对他们深表感谢。

我们将把这些意见运用到组织当中，作为首席执行官的动力，我们会仔细研究它们。我们会在此基础上提出一系列看法，说明我们将如何使用这些信息，以更好地促进 DNS 的安全性。下面，我把时间交给梅丽克 • 凯奥 (Merike Käo)，近一年半以来，他一直在负责协调这些工作。梅丽克 (Merike)，交给你了，有请。

梅丽克 • 凯奥： 好。非常感谢，约翰 (John)。今天的会议，这是会议的议程，我会简单介绍一下过去一年半以来我们所做的整体工作。然后我们将继

续深入工作内容，讨论 DNS 生态系统中的攻击向量、缓解措施，最后是建议，然后留出一些时间提问。每个部分都会由 TSG 的一名成员来讲述。请放下一张。下一张。

如约翰提到的，这项工作于去年 5 月开始，并且这是一项由 ICANN 首席执行官领导和实施的计划。这是履行他的承诺，即与社群合作，在安全和稳定问题上加强合作和沟通。这项工作主要旨在就 ICANN 可以和应该采取哪些措施来改进 DNS 安全性提供一些建议。另外还有，是否有 ICANN 特别不应该做的事情？请放下一张。

如约翰提到的，这项计划的大部分内容都是由于几年来发生了非常复杂的攻击而制定的。ICANN 意识到，过去对这些复杂攻击的应对都是临时应对。我们需要通过某种方式制定更多的结构，以应对整个互联网生态系统内的这些攻击，并研究在哪些方面需要提升合作和协作水平。请放下一张。

这张幻灯片展示了 TSG 的整体时间线。工作在 5 月开始，我们确定了 TSG 的成员构成。第一次会议于去年 6 月 16 日召开。夏季的大部分工作是确定范围和我们想要解决的一些主要问题。主要工作从初秋开始，一直持续到今年 5 月，第一部分的讨论围绕着攻击的根本原因和攻击向量展开。然后，我们制定了有关这些特定攻击向量的优先性列表，以明确哪些是较为严重而真正需要关注解决的。我们研究了既已存在或已经存在但还没有实施的缓解措施，以及可能缺失的缓解措施。然后，我们制定了草案文档。文档敲定并且制定出一些草案建议后，我们就向行业专家进行了一次技术咨询，然后编制了最终报告并于本周初发送给了跃然。请放下一张。

这是 TSG 的成员构成。这个工作组有九位成员。你们将看到，这是一个跨职能专家组，他们在 DNS 基础设施运营、安全事件响应、一般安全知识、注册管理机构/注册服务机构运营、国家/地区代码注册管理机构运营方面拥有丰富的经验和专业知识，并且拥有 CDN 和 ISP 经验。另外，他们还拥有深厚的 DNS 技术经验。所以，这个跨职能工作组的专业知识相当广泛和深入。请放下一张。

如我所说，我们还对草案文档进行了一次技术咨询审查，这些人提出了非常广泛的意见。TSG 对这次深入审查深表感谢，因为他们结合这次审查的意见丰富了最终报告和建议。请放下一张。

ICANN 也在多个层级提供了支持。这是 DSFI TSG 指导委员会，由四名董事会成员和两名高级职员组成。ICANN 在项目管理、沟通和技术主题问题专业技能方面为我们的工作提供了广泛的支持。毫无例外，我们有一位优秀的技术撰稿人，她凭借自己的技能将一个非常复杂的主题变成了一份报告，你在阅读这份报告时，会发现它的内容非常容易理解。请放下一张。

这张幻灯片讲的是全面 DNS 生态系统的广度和深度。我们预计这项工作需要一年时间，实际上用了一年半。这项工作是完全通过虚拟方式开展的，这带来了独有的挑战。我想以我个人名义感谢所有 TSG 成员和 ICANN 支持人员，因为，为了取得最终成果，我们召开了很多次会议，还有每两周一次每次持续两三个小时的工作坊。这是一个非常复杂的主题。我对我们提交的最终报告感到非常自豪。事不宜迟，我们开始讨论工作的实质，首先来看看攻击。请翻到下一张幻灯片。嘉文 (Gavin)，开始吧。

嘉文 • 布朗 (GAVIN BROWN)： 好的。谢谢，梅丽克。下面来看看我们研究的一些攻击向量，以及我们在分析中采用的方法。请翻到下一张幻灯片。

与梅丽克刚刚展示的幻灯片类似，这张幻灯片旨在说明我们研究的系统在威胁和针对它们的攻击向量方面的深度、广度或范围。我们会针对 DNS 端以及供应端进行介绍。这张图展示了从存根解析器到权威服务器的 DNS 解析路径中存在的要素，以及供应端存在的要素。所以，这包括作为注册人的最终用户、与注册人交互以提供域名的系统、注册管理机构和注册服务机构以及中间商（如分销商）之间的协议。目的是涵盖所有这些不同的系统，并研究可能威胁这些系统的所有不同的攻击向量。请放下一张。

我们经历的流程非常类似于风险分析，因为我们研究了各种可能的攻击向量，并尝试对它们进行分类，找出它们之间的共性。我们讨论了各种具体的攻击向量，把它们从我们在现实世界中经历的事件中提取出来。当我们在研究各个攻击向量时，我们考虑了有关哪些缓解措施可用（稍后我们会讨论缓解措施）、哪些方面存在差距的若干问题，考虑了是否对风险理解不全面，DNS 基础设施、DNS 系统本身是否特别容易出现互联网生态系统其他部分不会出现的特定类型的问题。下一张。

笼统而言，我们提出了很多攻击向量，我们把这些攻击向量浓缩成了你们将看到的这些。它们非常广泛，你们将会看到，某些攻击向量非常通用，因为 DNS 生态系统的参与者是组织，它们和其他方一样，都是组织和公司，他们与其他公司（无论是银行、洗车厂还是 gTLD 运营商）一样面临着同样的安全挑战。某些攻击向量是专门针对 DNS 以及系统中的参与者使用的协议和系统的。所以，你们会看到，我们涵盖的内容包括 TTL 的选择，以及基础内容，比如你的密

码策略有多好等等。这些内容进一步浓缩成了我们将在下一张幻灯片上介绍的向量。我们可以继续来看下一张幻灯片。

这些方面浓缩成立这些类型的攻击向量。我们会更详细地讨论部分内容，首先来看看比较通用的那些方面。身份和访问管理是一种较为通用的安全挑战。每家需要使用电脑的公司都会考虑这个问题。访问控制和授权也是如此。这些是专门针对 DNS 系统的一些方面。但是，诸如资源模拟、拒绝服务问题以及漏洞问题，无论是在代码实现中还是在协议本身中都会存在。我们在构建基础设施时所做的选择会导致系统易受攻击，而这可能是你不希望出现的。请翻到下一张幻灯片。

首先是第一点，身份和访问管理，凭证在整个基础设施和供应系统中随处存在，在权威系统中也是如此。凭证用于在参与者之间的互动中进行身份验证。如果你是注册管理机构的雇员，你将使用某个用户名或密码登录有关注册管理机构的管理系统。如果你是注册服务机构，你将使用某个用户名和密码访问注册管理机构的 EPP 系统。如果你是注册服务机构的雇员，你将使用你的用户名和密码访问它们的系统。一直到最终用户，都是如此。在该系统的任何一点上，这些凭证都可能被盗用。参与管理这些凭证的组织必须做出有关实施政策的决策，以保护凭证免受你可能看到的各种攻击 — 密码喷洒、密码重用、网络钓鱼等等。这是我们在此方面的工作重点，特别专注于注册人的凭证，注册管理机构、注册服务机构和分销商之间的身份认证，以及使用被盗用的凭证通过冒充注册人和注册管理机构之间链路中的一个实体来发起与注册管理机构的交易的威胁。请放下一张。

这是访问控制授权不充分的一个示例。这实际上与子域接管有关。这是一个记录存在于域名中的场景，该域名具有指向其他资源的别名或 CNAME 记录。这使攻击者可能控制该域名，而无需过多验证攻击者是否真的是域名所有者。请放下一张。

下一个攻击向量与资源模拟有关。攻击者可以通过这种方式使 DNS 查询重定向至第三方。这种定向可能产生若干不同的影响，具体取决于发生在系统中的哪个位置。所以，有时候这可能作为合法使用的一部分进行。捕获门户是一个非常常见的地方，在这里，网络会截获打算退出网络的 DNS 流量，以便向用户提供捕获门户的登录表单。但是，它也可能是恶意活动的结果，例如，通过在网络上主动拦截，在计算机或最终用户设备上安装恶意软件。所以，其他一些方式可以通过模拟递归解析器来实现，通过模拟权威服务器，即递归服务器位于最终用户和权威域数据源之间。

相似域或传真域。这与你们所说的有点不同，这不仅仅是网络钓鱼，而是有些不同，因为在这种情形下目标是基础设施的用户而非消费者服务的最终用户。欺诈颁发的证书和根操纵也被视为此攻击向量的一部分。转到下一张幻灯片。

这是我们所说的传真域的一个示例。单应攻击是这种形式的攻击向量最明显的例子。

我们讨论的下一个攻击向量是代码和协议中的漏洞。当 DNS 软件出现问题时，我们在处理这两种不同类型的漏洞时存在不同的问题和挑战。一般来说，缓解代码漏洞的方式明显不同于缓解协议漏洞的方式。因为当 DNS 协议出现问题时，正如我们所看到的，不是最近出现的问题，而是围绕 SADDNS 以及最著名的 Kaminski 攻击等问题

出现了许多漏洞。更改协议会影响互用性。如果你在没有与所有运营商和实施者仔细协调的情况下更改协议，那么你就面临着破坏系统稳定性的风险。但是，它们确实需要得到解决，并且它们会对易受攻击的系统产生负面影响。如大家所见，缓存中毒之类的事情在协议漏洞的情况下尤其可能发生。下一张。

这是说明缓存中毒原理的例子。你们将会看到 — 我认为这里缺少了箭头。可以看到它们吗？我们开始吧。它们在下一张幻灯片上是可以看到的。

递归服务器接收来自最终用户的查询，它们在寻找 icann.org，在递归服务器收到来自权威服务器的答案之前，主动攻击者能够拦截该查询或将欺诈性欺骗响应发送回递归服务器，从而使得在递归服务器从正确的权威服务器收到合法响应之前，将欺骗性答案发送给最终用户。转到下一张幻灯片。

基础设施选择。这些是 DNS 系统或 DNS 服务的运营商做出的决定，它们可能会对域名系统的安全性和可用性产生意想不到的后果。TTL 就是这方面的一个很好的例子。显然，我们在这里把长 TTL 和短 TTL 都列为了问题。实际要表达的就是，Goldilocks TTL 不能太短，不能太长，而是要恰到好处。这些是短 TTL 有用和适当的情境。这些是长 TTL 有用和适当的情境。但是，意想不到的后果意味着，你需要进行仔细的风险评估，确保决定产生的后果不会反过来对你产生不利影响。请翻到下一张幻灯片，这里会对此进行说明。

这里描述了一种情境，TTL 已在权威服务器上的记录中实现。该 TTL 确保最终用户将继续在该 TTL 的空间内接收查询或查询的答案，因为缓存记录将由解析器提供。但是，如果攻击者能够通过劫

持域名或我们在本节中讨论的其他向量来拦截查询，那么恶意答案将在这段时间内被缓存，在记录过期并且可以从权威服务器检索正确答案之前，用户仍然容易通过该 TTL 被利用。下一张。

我们将 DNS 作为攻击向量本身进行了讨论。这主要不是围绕数据泄露和使用 DNS 作为隐蔽通道，等等。DNS 通常允许在不被过滤或阻止的情况下传输和退出网络，并且这正以多种不同的方式被利用，从而允许攻击者渗透系统或将数据从该系统泄露到外部。请放下一张。

最后，我们讨论了拒绝服务。这对于任何关键 DNS 基础设施的运营商来说都是一个持续和压倒一切的挑战和问题。由于 DNS 协议的运作原理，使用 UDP 意味着 DNS 服务容易遭受欺骗攻击，它们容易受到放大攻击和反射攻击。对 DNS 提供商的拒绝服务攻击可能破坏更多组织的工作，如果拒绝服务攻击的目标是注册管理机构或注册服务机构服务的根服务器的运营商，而不仅仅是最终用户，就会发生这种情况。请放下一张。

我们对攻击向量的概述到此结束。下面请我的同事来介绍缓解措施。杜亚尼 (Duane)？

杜亚尼 • 韦瑟尔 (DUANE WESSELS)：

大家好。我是杜亚尼 • 韦瑟尔，下面我向大家介绍缓解措施以及我们的报告。请放下一张。

嘉文刚刚介绍了一些攻击，我们在工作组中也讨论了缓解这些攻击的方式，我们提出了许多不同的缓解措施。有些内容没有写进最终报告中，我在这里仅仅介绍写进了报告中的措施。下一张。

在工作组中，我们用了大量时间讨论身份认证，你们可以看到，许多建议和缓解措施都是围绕访问控制和身份认证的。人们可以采取的最佳行动之一是，使用复杂密码来保持 DNS 的安全。有许多例子表明，过于简单的密码会导致盗用。与使用复杂密码类似，人们可以使用一次性使用的凭证或多重要素验证。当然，随着我们的凭证和密码变得越来越复杂，有必要使用某种类型的密码管理器，由密码管理器帮你记住密码。

我们讨论了风险意识，这是指要意识到凭证可能通过不同的方式被盗用，例如网络钓鱼攻击。我们讨论了可以防止弱密码的服务的可用性和使用。例如，可能编写一些代码，告诉你某个密码是否足够强或是否有一定的强度要求。你还可以查看建立的已知被盗用密码的数据库。假设攻击者也能访问这些数据库始终是一个好主意。你不会想使用已经在别处被盗用的密码。

我们讨论了在发生攻击的情况下有哪些补救解决方案。最后，我们讨论了潜在客户在提交服务请求时，可以通过哪些方式对域名和注册人进行验证和确认。请放下一张。

可用性、完整性和隐私方面的缓解措施。其中一些已经是众所周知的了。对于可用性，我想很多人都知道单点故障是一个非常糟糕的主意。通常，我们会从网络和网络服务的角度来考虑这一点。例如，不要将所有 DNS 服务器放在同一个网络或同一个数据中心。但是，你可能会想到其他类型的单点故障，例如，仅使用一种软件甚

至一种硬件，等等。此外，大家知道，在众所周知的 Dyn 攻击中，如果你使用的是辅助 DNS 服务，那么将它们分布在不同平台上通常是一个好主意。因为，如果你使用单一平台，而该提供商出现故障，那么你就可能面临糟糕的局面。

在完整性方面，最好的缓解措施之一当然是 DNSSEC 签署域并在发布端和解析端实施 DNSSEC 以实施验证。如果你可以使用，注册管理机构锁和某些类似产品是防止域名劫持的好方法。我们还讨论了一些较新协议的使用，例如 CDS、CDNSKEY 和 CSYNC 协议，它们使在子区域和父区域之间传输 DNSSEC 材料变得更加容易。

在隐私方面，显然，最近开展了大量关于使用加密 DNS 传输的工作。我们开始看到这种情况越来越多，这是实现 DNS 隐私的一种非常好的方式。请播放下一张。

人们应该知道的其他缓解措施包括监控。你可以订阅品牌保护服务。例如，如果你公司的品牌商标和域名在另一个注册服务机构或顶级域下注册，你会收到提醒消息。这可能是你想知道的事情。证书透明度是一个让人们可以看到 SSL 证书请求的项目。项目中提供多项服务，如果针对你的域名发布了证书，你会收到提醒消息。如果证书不是你本人发布，那么这可能是你想要知晓的情况。

认证机构授权记录，简称 CAA 记录，你可以将此记录放入你的区域，它指定了哪个认证机构可以发布关于你的域名的证书。考虑这项服务是个不错的主意。

在路由 RPKI 和路由源方面，身份认证公告有助于保护你的网络不遭受虚假广告的影响。你也可以对此进行监控。

如果组织需要对传递到网络的数据进行任何类型的检查，它们可能需要考虑使用针对深度包检测进行了优化的路由器或交换机，这些路由器或交换机还可以窥视这些数据包，告知人们通过网络传输的内容。

对于软件开发者，我们讨论了需要制定良好软件开发生命周期实践。这只是软件开发的一种标准方法，它引入了保持软件最新、已打补丁和已进行测试的最佳当前实践。我可以肯定，大家都知道定期为软件打补丁很重要，不仅从用户角度来看是这样，而且从开发者角度来看也是如此，这样做可以保持补丁最新并在发现问题时予以解决。请播放下一张。

与访问控制有关的缓解措施包括使用基于行为的访问架构。例如，“零信任”就是其中一种。这项措施近来受到大量关注。对关键服务进行分区始终是一个好主意。例如，将 DNS 服务与电子邮件服务、Web 服务分开，把它们放到不同的系统中，这样即使其中某个服务受到攻击，也不会影响其他服务。当然，应该考虑对更敏感的帐户进行更严格的访问控制。

特别是在你能够对服务进行分区的情况下，仅将数据服务的访问限制在 DNS 端口是个好主意。这是端口 53，现在使用 TLS 的端口 853，也许是使用基于 HTTPS 的 DNS 的端口 443。如果你运营 DNS 解析器，这不是设计供第三方使用的，你应确保它有适当的访问控制，可以将其使用限制在应该使用它的用户范围内。请播放下一张。

有关端点和网络控制的指示。防病毒软件已经存在很长时间了，并且对许多用户来说仍然非常重要。我们没有在报告中花费大量时间来讨论抗病毒软件，但是有简单提到过这点。严格控制 DNS 解析器

的选择意味着，如今许多设备从网络、DHCP 服务器接收信息，TCP 服务器会告诉它们使用哪个解析器。这通常有效，但是恶意软件或其他攻击向量也可能更改某个设备已经分配给其他设备的递归名称服务器。网络运营商希望关注这点。可以在防火墙上阻止未经授权的 DNS 解析器，也可以执行其他检查以确保设备使用的 DNS 解析器正确且适当。当然，对于能够保护其用户的组织来说，DNS 防火墙是一个好主意，可以真正确保这些用户只访问适当且安全的目的内容。请播放下一张。

我们在报告中讨论的缓解措施就分为以上几个类别，我都已经介绍完毕。其中的一些缓解措施包括凭证挑战、用户帐户的访问控制等等。嘉文谈论了资源模拟，以及代码和协议漏洞。报告讨论了使用 DNS 作为攻击向量与使用 DNS 作为目标的问题。当然，还有拒绝服务攻击和事件响应机制。这就是我的最后一张幻灯片了。下面我把时间交给马克 (Marc)。

马克 • 罗杰斯
(MARC ROGERS)：

你好。我的麦克风开不了。好的。下一张。我要介绍的是在工作组讨论中提出的建议。这些建议与所讨论的攻击向量和缓解措施有着明显的联系。建议大致分为以下五个方面：运营改进、研究、合同、资金以及教育和意识。下一张。

提出的第一条建议是，ICANN 应该与 SSAC、GNSO、ccNSO、TLD-OPS 等组织合作，编制桌面演习计划。通过这项计划，应努力创造机会在类似事件的情况下行使运营职能，确定可能出现的运营差距。通

过持续采取此等行动，ICANN 和其他机构可以识别、记录和跟踪这些运营差距，以便在将来的建议中进行处理和标记。下一张。

在此方面提出了几条研究建议。第一条是关于 DNS 滥用。威胁形势从来都不是静止不变的。它总是不断演变，DNS 滥用也是如此。昨天的滥用技术发生演变，成为明天的新滥用技术。随着不同技术的部署或不同 DNS 架构的部署，新的途径也在开辟。所以我们的建议是，我们应该继续深入研究 DNS 滥用，以确保我们始终了解当前的滥用形式、滥用发生在何处，从而使我们能够先发制人。

下一条建议是，我们应该调查 DNS 安全增强措施。由于威胁形势在不断变化，因此 DNS 安全增强措施也在不断变化。我们认为，应该制定一个计划来调查各项 DNS 安全增强措施的限制、风险和益处。在报告下文中列出了若干这些增强措施。总体想法与滥用类似，我们需要保持先发制人，我们需要继续监控它，并需要创建一个反馈循环，找出差距，确定改进，并不断反馈回去。

结合前面几个部分中有关身份验证的讨论，我们认为应该对适当的身份验证最佳实践进行调查。我认为，ICANN 应当与其他相关的组织社群一道，针对面对 DNS 的不同角色和风险应视为身份验证最佳实践的内容开展研究并编制报告。下一张。

合同方面的建议是，ICANN 应努力向签约方机构授权，使其能够在切实可行的情况下对域注册系统和权威名称服务采用安全增强措施。我们认为，这样做可让我们确保并向组织授权，使其能够执行此等更强有力的 DNS 安全措施。

下一条建议关注的是漏洞报告奖励计划。这是工作组内的一个活跃话题，因为大家围绕应在哪些方面提供漏洞报告奖励、有效性如何

以及应该如何采用提出了许多意见。我们一致同意的是，ICANN 应该主导开展 DNS 漏洞报告奖励计划的可行性研究。因为有许多方面，例如，DNS 基础设施并非由特定组织所有，或者 DNS 基础设施不再维护，在这种情况下，制定一个托管的漏洞报告奖励计划，专注于这些方面和这些软件来识别漏洞将是有利的。现在，因为这是一个非常具有挑战性的话题，我们认为最佳方法是对此进行可行性研究，以考虑最佳方法，考虑最具成本效益的方法，并考虑如何将由此产生的漏洞转移到正确的实体以确保它们得到切实解决。下一张。

我们认为，在教育和意识方面采取行动很有必要。我们认为 ICANN 应该努力构建并沟通教育计划，鼓励 DNS 利益相关方根据适当的标准，为所有应该进行身份验证的互动制定身份验证机制。并且要对那些存在与弱身份验证方案相关风险的利益相关者进行教育，告诉他们有太多的旧有身份验证只是出于无知而被利用。我们认为，通过教育和意识方面的措施，我们有很大的机会可以推进制定更强大的身份验证方案。

注册管理机构锁。ICANN 应该努力改进注册管理机构锁功能的文档记录和理解，促进其在适当情况下的使用，并加强有关“注册管理机构锁”和“注册服务机构锁”之间差别的理解。注册人应该能够找到这些功能提供什么、不提供什么以及它们之间差别的明确定义。ICANN 还应考虑促进对注册管理机构和注册服务机构服务的最低要求进行标准化。下一张。

我们认为，需要提升对基础设施安全方面的最佳实践的意识。ICANN 需要开展方式和善举等计划，以衡量和报告它们的采用情况，并使用报告来锁定教育材料，以提高对基础设施安全性的认识。

ICANN 应该采取从这些计划中得出的最佳实践，并确保签约方机构和 ICANN 社群知晓这些最佳实践。如果不存在最佳实践，ICANN 应该努力鼓励开发和部署这些实践，并推广 DNS 安全功能的采用，在整个 DNS 生态系统中宣传这些功能。例如，DMARC、SPF、TLSA、DANE、DNSSEC 等等。

接下来是有关 DNS 阻止和过滤的建议。ICANN 应该编制信息丰富和富有教育意义的材料，帮助 ICANN 社群、签约方机构和其他相关方了解出于安全性和稳定性原因在全球 DNS 社群进行 DNS 阻止和过滤的风险与益处。下一张。

在事件响应方面，ICANN 应该与所有相关方一道，鼓励在整个 DNS 行业中开发和部署正式的事件响应流程，以便与生态系统中的其他方进行互动。此等工作包括事件响应处理以及以受保护的方式分享威胁和事件信息。这也可以与桌面演习相结合，以确保可以在操作功能的任何缺口中制定任何此等事件响应计划，便于识别。

建议 E6，这是隐秘的通道意识。ICANN 应该发布有关使用隐秘通道作为攻击向量的教育材料，这可能被视为对 DNS 本身的滥用，因此需要处理其他 DNS 滥用问题。下一张。

如果说我们可以从建议中选择两个最优先的建议，我们认为首先应该是建议 R3，调查适当的身份验证最佳实践。第二是建议 E5，事件响应。下一张。

好的。交给你了，梅丽克。

梅丽克 • 凯奥： 好的。非常感谢。如果你们想了解更多有关技术研究组的信息，了解章程中的内容，查看范围界定文档、工作计划时间线、会议议程和记录以及其他资源，请访问网站。如约翰刚刚提到的，报告会在下周某个时间与一篇博客一起发布。我提前告诉你们，网站上有很多内容，比我们在会上短时间内能够介绍的内容更为详细。网站上发布了许多很好的内容，你们会发现这些内容非常宝贵。我真切地希望 ICANN 首席执行官会评价这是一份宝贵的报告，那么我们就可以根据报告采取行动了。现在是我们的提问时间。目前我在问答窗格中没有看到任何问题。

温迪 • 普若菲特： 我认为，所有在问答窗格中提出的问题都以书面形式回答了。

梅丽克 • 凯奥： 是的。大家是否还有任何新的问题，如果有，请在问答窗格中写出来，我们很乐意回答。好的。问题又来了，“可以在哪里查看最终报告？”最终报告将在下周与博客一起发布。我相信大家也会访问我刚刚指出的维基网站。这个问题是，“这些问答是否会随录音一起提供？”我把这个问题交给工作人员来回答。是否会随录音一起提供文稿？

温迪 • 普若菲特： 让我向 MTS 团队核实一下。

梅丽克 • 凯奥： 好的。非常感谢。唐娜 (Donna)，谢谢你提出这个问题。我的意思是，正如你们所知，在过去的 18 个月里，我们在这项工作中投入了很多时间，也运用了许多跨职能专业知识。这真的非常棒。我想感谢对这份报告做出贡献的每一位成员。

现在，我看到没有人提问了。如果大家没有问题了，我想在此感谢参加本次筹备会议的每个人。请大家在下周报告发布后查阅报告，了解报告的内容。

温迪 • 普若菲特： 问答窗格中还收到了一个问题，“攻击者的主要动机是什么？他们的原籍国在哪里？”

梅丽克 • 凯奥： 我来回答这个问题。TSG 的成员也可以进行补充。攻击者的动机各不相同。攻击者可能只是个人，也可能是有组织的犯罪，实际上，攻击者可以来自任何民族国家。这就是我们当今所生活的虚拟世界的本质。好了，我们的会议到此结束。非常感谢大家的参与。

[会议记录结束]