圣胡安 — KSK 轮转最新信息
2018 年 3 月 14 日星期三 — 大西洋标准时间 16:15 至 16:45
ICANN61 | 波多黎各圣胡安

发言人（姓名不详）： 大家好，我们的根区 KSK 轮转会议马上就要开始了。能否把演示文稿显示在屏幕上？

我们将在 30 秒后开始会议。

大家好，欢迎参加根区 KSK 轮转会议。希望今天参加会议的人没有在本次 ICANN 会议期间看到过我讲解这个内容。我们来看看这里。我首先向大家概述一下我们今天会议的议程，我认为，如果你有足够的兴趣参加今天的会议，那么你就应该知道，根区 KSK 轮转最初安排在 2017 年 10 月 11 日进行，但是我们后来决定推迟这项行动。[听不清]分析了我们的 CAD 145 信任锚报告数据，他们发现大约 7-8% 的解析器（这在当时是一个相对较少的数量）报告称其只有我们所说的 KSK 2010，或者当前返回的 KSK 没有新的根区 KSK。这些 7-8% 的解析器提供了一些不正确的信息。ICANN 首席技术官办公室研究团队对来自不同根服务器的流量反复进行了分析，结果发现本质上是一回事。根据你查看的具体时间，百分比会高些或者低些。这个百分比与我们满意的比例相比仍然较高，更重要的是，我们不知道为什么这些解析器会报告旧密钥。我们决定暂停根区 KSK 轮转并尝试确定这些解析器报告旧密钥的原因。我们获取了一个列有 500 个解析器的列表，这些解析器在 2017 年 9 月

只报告了旧密钥和 KSK 2010，我们尝试对这些解析器进行追踪，发现只根据 IP 地址追踪运营商很困难，我们知道这点，这是出现那种现象的存在性证明。我们只能接触这些解析器中的 20%，也就是大约 100 个地址，大多数位于虚拟机或容器等临时托管处所知的 IP 范围内。

RFC 8145也存在一个问题，信号本身是作为 DNS 查询发送的，所以这意味着它执行的操作就像从一个解析器转发到另一个解析器一样。我们知道正在进行转发，这掩盖了信号，你可能会认为一个特定的解析器只有 KSK 2010，解析器可能是正常运作的，它可能是后面向它转发的解析器，并且报告称只有 KSK 2010。

这里的结果是没有证据确凿的单一原因，如果有一两个根本原因则会比较理想，这样我们可能会与供应商讨论以修复我们发现的缺陷，我们可以调整我们的通信信息，但事实并非如此。由于这项研究没有提出清晰的前进方向，因此 ICANN 组织决定向社群征求意见。

现在我们来看看 2017 年 12 月底。我们说过，我们会接受 ICANN 组织名单上进行的关于 KSK 轮转的意见和讨论，该名单专门用于这个项目的更新和讨论。如果你没有在那个名单上，我建议你加入进去。这个数量现在非常低，但是对于这个项目[听不清]。讨论的结果是，人们普遍认为这里确实没有很好的衡量标准。ICANN 在两年前组建了设计团队，该团队编制了有

关如何轮转返回的 KSK 的报告并提出了建议。他们指出，良好的衡量标准是受影响的用户人数，如果根区 KSK 轮转之后受影响的用户达到 0.5%，则表示存在足够多的问题，应该进行回退。如果是用户人数，这是非常合理的衡量标准，但是这也是非常困难的衡量标准，并且这不是 RFC 8145 数据向我们提供的信息。关注这方面的人们希望将来能确定出更好的衡量标准，他们期待的衡量标准是现在所说的 Sentinel，这是来自 Google 的沃伦 • 库马里 (Warren Kumar) 和[听不清]正在努力制定的草案，它将允许进行用户群衡量，但是目前还没有采用。这个团体中的共识性意见是 ICANN 应该及时进行密钥轮转，并继续开展我们一直在开展的外展。

根据 2 月 1 日的反馈，我们发布了一份计划草案，我想强调的是，这是一份关于 KSK 轮转的计划草案。这个计划的要素包含，首先我们会将其推迟 1 年，我们将在 2018 年 10 月 11 日进行轮转，我们希望关于名单的讨论可以产生出衡量标准，我们并没有让任何人建议任何特定的标准。我们还将继续开展外展，这些工作包括我们现在召开的会议，公布 KSK 轮转等等，我们还将发布更多关于信任锚数据的观察意见，主要是 RFC 8145 数据，尽管我们会继续开展相关工作，但是我对这些数据实际告诉我们的信息却越来越缺乏信心。我不确定数据是否真的告诉了我们有用的信息或者是否为我们提供了与项目并不真正相关的报警信号。

这里有一个重要的一点是，我们有一个正在进行的公共评议期，这份计划只是一份草案，是向社群征求意见的一个主题。我们真的希望听取社群的意见，获得他们对于提案的反馈。公共评议期将于 4 月 2 日结束，幻灯片的下方有网页的网址。如果我们最终决定继续按照计划进行，现在提出的是时间表和计划，计划草案是像这样的文件。公共评议期于 4 月 2 日结束。就像任何一次 ICANN 公众意见征询一样，需要在 4 月中旬发布工作人员报告。我们还将是需要修改计划并进行发布。如果你现在熟悉了 ICANN 董事会会议的节奏，就会知道 ICANN 董事会每年召开 6 次会议，在每届 ICANN 会议期间召开会议，所以会在 ICANN 会议期间召开 3 次会议。然后，在每两届 ICANN 会议之间，董事会会举行所谓的董事会工作坊。下届 ICANN 董事会会议将在 5 月中旬在董事会工作坊期间举行，届时我们将请董事会做出决议，要求 ASAC 以及我们的 SAC 在 10 月 1 日之前审核计划并提出意见 — 我还没有更新这些幻灯片。我们可能会在巴拿马举行另一场会议，谈论与根区 KSK 轮转有关的问题。我们希望能在 10 月 1 日收到 ASAC 以及我们 SAC 的反馈，我们将根据反馈对计划进行修改。如果这些修订没有要求改为 2018 年 10 月 11 日之外的日期，那么我们将在 8 月中旬发布最终计划，并在 9 月的董事会工作坊上请董事会做出决议，指示 ICANN 组织于 10 月 11 日对密钥进行轮转。

这就是我们目前所处的状态，这就是我们前进的方向。我希望再次强调，我们非常希望获得社群的反馈，希望人们能在公众

意见征询期间参加讨论。我想发送剩余的演示文稿，这部分演示文稿讲述的内容是我们获得的信号，我们通过这份 RFC 8145 信任锚报告获得的数据。

目前，ICANN 首席技术官办公室访问了 RFC 8145 数据，事实上，基于 12 台根服务器的主要突破性发展，这张幻灯片现在已经过时了，我们在向我们提供数据的服务器的列表中增加了 H。2017 年底进行的初步分析使用了来自 B、D、F 的[听不清]数据，但是自那时以来我们一直都在使用[听不清] DNS 上限的插件。根服务器运营商运行 DNS 上限并分析了实时流量，每隔 60 秒，这个插件就会分批编制一份它所看见的统计数据的报告以及一份它所看见的信任锚的报告。它将它们作为 DNS 查询发送到 ICANN [听不清]运营的区域，这种做法很聪明。你们可以看看报告的样例，这里是时间戳，这里是由破折号而不是点分隔的源 IP。信任锚用四位十六进制数字表示，4A5C 是 KSK 2010，4F66 是KSK 2017。你会看到一个备注 ID 和一个根服务器 ID。基于这一切，我们可以编译这个图。你们可以看到随着时间的推移，我们正从更多的服务器获取越来越多的报告。让我来解释一下这幅图，因为它乍一看可能并不完全明显。这三条线绘制了两种不同的东西。红色和绿色线条绘制的是报告 8145 数据的 IP 数量，你们可以在左侧轴上读取源的数量。你们可以看到随着时间推移的变化，在这里看看绿色的线，这是报告信任锚数据的源总数。每天的源都是独一无二的。此时大约有 50,000 个独特的 IP 地址每天向我们报告信任

锚。红线指的是报告它们只有旧密钥的解析器的数量。如果你用红线数字除以绿线数字，就可以得出一个百分比，这个百分比绘制在黑线上，你需要读取右侧 Y 轴的刻度，你可以看到现在我们有大约 20% 的解析器报告说它们只能报告旧密钥。请注意，1 月出现了大幅上涨，当时我们突然获得了更多的人员报告，并且百分比数字变得更糟。我们可以确定的是，这是升级为 Unbound 造成的结果，Unbound 168 于 1 月中旬发布，所以时间非常契合，这项发布的目的是处理一项安全漏洞，所以我们的假设是由于这是一个与安全相关的补丁，因此人们会积极地升级为 Unbound。但是，30 天后 KSK 2010 报告的数字并没有下降。

如果某人升级为 Unbound 并且没有运行 Unbound 信任锚工具，换句话说，如果某人升级为 Unbound 并且运行 Unbound 信任锚工具，他们将立即使用正确的数据更新自己的信任锚存储并将拥有 KSK 2010 和 2017。常见的做法是升级但不运行 Unbound 信任锚，因此这就意味着你拥有的 Unbound 版本仍然配置的是旧密钥，但是如果其在 30 天之后适当地通过 RFC 5011 进行报告，它就应该运行这个流程并意识到应该配置 KSK 2017。这为什么还没有发生呢？一种假设是，如果这些是临时虚拟机或容器，你可以想象为其中一种，拥有旧密钥，通过 RFC 8145 报告旧密钥，我说的是旧密钥，我应该严格地说是 KSK 2010。它报告 KSK 2010，它运行几小时、几天，它停机了。它从来没有时间完成 RFC 5011 [听不清]下次重新开始

时，它从头开始，它仍然只有 KSK 2010，它只通过 8145 报告 KSK 2010，并重复这个过程。在某些时候我们需要进行进一步的分析，你需要停止制作你的幻灯片然后乘飞机前往波多黎各进行使用幻灯片进行演讲，这就是我们现在正在做的，我们需要持续做的事情之一是审查特定 IP、它们的发生频率、报告频率。我们知道，Bind 和 Unbound 以一种非常固定的节奏发送这些 8145 报告。如果我们看见 IP 没有这样做，一个合理的假设是，它们[听不清]在不断地上升和下降。这可能不是唯一的原因，但是这是为什么我们要进行研究试着弄清楚这个问题。

这里是针对各个根服务器的图表，这些图表是相同的，因为这个图表是针对根服务器的，那时候这些图表是针对 11 个为我们提供数据的根服务器的。你们可以看见数据，不同的服务器可以在不同的时间段为我们提供数据。你们看看图表就可以发现，它们都是类似的，区别在于 J 根，它的报告百分比较低，因此 J 根看起来比其他根都更好。至少在百分比方面是这样的。[听不清]报告称，我们没有获得来自所有 J 根实例的报告，因此可能对此有影响。这里的要点是，根服务器之间没有真正大不相同的数据。我认为有趣的是 1 月中旬当我们看到大幅增长时发生的行为变化。这张图表显示了每天增加的独有 IP 地址，这里的数据点代表了当天有多少个我们之前从未看到过的源在向我们报告数据。大家可以看看从左到右的读数，我们一直非常活跃，看起来似乎从没超过 1000，每天有几百

个新的 IP。1 月发生这项假设的升级事件之后，我们现在每天都会看到更多独特的源在发送报告。大约 15-16,000 个。如果你要绘制一张展示我们每天看到多少个累积的独特 IP 的图表，那么就应该是这张。绿线显示了在任何给定的时间点，我们看到了多少个 IP 地址。显然，在早些时候，也就是从左边开始时这个数字很小，随着时间的进一步推移，我们看到了更多的独特 IP 地址，目前这一数字是 730,000。截至目前，我们拥有 730,000 个不同的 IP 地址，我还没说这是演示文稿，这是 V4 和 V6 地址的组合。大约有 730,000 个 IP 地址向我们报告数据，其中有大约 250,000 个 IP 地址在某些时候报告称它们只有 KSK 2010。你们看看我们目前拥有的累积数字，就可以知道关于这项计算的数学含义变得更糟糕了。我们从未见过的地址总数中有大约 35% 的地址报告称只有 KSK 2010。

我决定通过“斜杠 24”来考虑这个，所以你们可以看到这个图形的形状稍有不同。在 1 月出现增长之后，这是新的“斜杠 24”中出现的大幅增长，然后逐渐减少。如果我绘制一张累积图表，就可以看出我们仍然有许多“斜杠 24”。我们来看看绿线，它最后达到了大约 350,000。这是平均数，我们在这里损失了大量解析，平均每个“斜杠 24”2 个 IP。我希望这个数字能变得更小，这就可以表明可能存在拥有一大群地址的整块，我们可以调查这些块，对此的良好假设是也许它们是只拥有动态临时机器的地址栏。

那是许多地址，有趣的是，报告 KSK 2010 或 KSK 2010 和 KSK 2017 的这些地址的总数，这个数字大于独特 IP 的数量之和。这就意味着有源在报告称其只有 KSK 2010，然后它们报告称自己有 KSK 2010 和 KSK 2017。并不一定按照这个顺序，但是它们发送了两项报告。可能的一个原因是，想象有一个源在报告 KSK 2010，一段时间之后它们又在报告 KSK 2010 和 2017。一个原因是机器进行了升级，但这不是唯一可能的原因。它现在拥有了新的 KSK，但是在这 750,000 个 IP 中只有大约 1550 个在发送两项报告。这就意味着，我们不能指出大量机器并说，一种假设是它们进行了升级。问题的一部分是 8145 信号真的存在问题，如我之前所说，我们知道这里涉及到了转发器，所以只是因为你看到了来自一个源 IP 的报告，但你不能保证那就是你所看到的源 IP 配置。这可能是其他人在转发体现他们 IP 配置的 8145 报告，这份报告然后转发至一个根服务器，并且被我们看到。这是对于为什么你会看到报告 KSK 2010 以及 KSK 2010 和 2017 的单一源的另一种解释。

我们还知道至少有一种版本的实施会报告 8145，即使它并没有进行验证。如果它拥有 KSK 2010，那么这也没关系，因为它会进行 DNS 验证并将其用作其配置的一部分。它是针对它进行配置的，但是没有关系。

如果你们想自己看看这些图表，我们会每周进行更新，这是网址。Root trust anchor reports 点 ICANN 点 org。我才刚刚开始以这种方式对数据进行交叉分析，这是基于这个特定的表格，

不是基于目前仅报告 KSK 2010 的全部 250,000 个 IP。这是基于一个较少的数量，我不记得总数是多少了，一下想不起来。这是考虑的每个自治系统的源数量，然后进行反向排序，因此 IP 报告最多的 ASN…请原谅，这不仅是 KSK 2010，这是所有自治系统编号报告。如果只有 KSK 2010，那应该是另一张图表。这就意味着，我需要再次运行这个，只考虑 KSK 2010，它将允许我们进行一些联系尝试，了解拥有只报告 KSK 2010 的最大数量解析器的 AS 的情况。

我们已经分发了一份只向 ISPCP 和 RAR 报告 KSK 2010 的 IP 地址清单，目标是双重的。其中一个目标是使这些系统升级，但是我们仍然非常有兴趣了解这些系统未升级的原因。如果我们了解到了，比方说，最好的结果之一是了解到的确存在地址空间，这里有许多[听不清]机器刚好在运行只有 KSK 2010 的旧配置。这可能会是一项积极的发现。这张幻灯片现在已经过时了，我的确获得了 ICANN 内部权力机构的授权来公布这份清单。我们将会发布一个页面，看起来就像这个一样，我会根据 ASN 按相反的顺序排序，你可以点击 ASN 并获得一份只报告 KSK 2010 的 ASN 的地址列表。很快，运营商了解它们网络的运行状况就会变得更加容易。显然，到那时我们将首先接触拥有最多只报告 KSK 2010 的地址的运营商，并尝试了解发生的情况。后续步骤是，继续尝试弄清这个 8145 数据的情况，我对它提供的信号不满意，但是这是截至目前我们拥有的唯一数据。要做的负责任的事情是继续调查，尝试弄清它告诉了我们

什么，如果我们确信它事实上并没有告诉我们任何有价值的信息，那么这本身而言就是一项积极的发现。我们将尝试联系报告大量只有 KSK 2010 的解析器的网络，我们将帮助其他人进行调查。我们将继续讨论这个问题，所以你们会继续看到我和我的同事们，我们将继续倾听社群的意见，因为如我之前所说，你们能够提供帮会的方式就是对计划发表意见，这里是网址，请加入 KSK 轮转名单随时了解最新信息。下面，我很乐意回答大家提出的任何问题。我们还有一点时间，之后我们就将进行下一个事项，第 5 点。

霍华德 • 本 (HOWARD BENN)： 我是霍华德 • 本，来自三星电子。我想提出的问题与那张列有所有运营商的幻灯片有关，就是这张。我的猜测是依赖地理网络，这可能是他们的 LTE 网络完全在虚拟机上运行，并且几乎无疑会永远达不到 30 天的限制。非常有趣的是看到大量移动运营商在那里，无论他们是否遭遇了同样的问题。我很乐意提供一些地理联系信息，因为这些设备是我们的。

发言人（姓名不详）： 好的，谢谢。

马克 (MARK)： 我是马克[听不清]，来自 ISP，但是我仅代表自己发言。我们转到第 4 张幻灯片吧。就是这张。我看到幻灯片的底部写着讨

论结果，我对第一点和第三点有些疑问。我用我自己的话来说，你可以告诉我我是否理解错了。第一点说的是，我们不知道这会对互联网产生什么影响。第三点说的是，不管怎样都要做。我是否误解了其中的意思？

发言人（姓名不详）： 这是悲观者的理解。

马克： 你能为我进行乐观的解读吗？

发言人（姓名不详）： 我认为这个演示文稿的其余部分就是乐观的解释。我来进行认真的回答。认真的回答是，这是一个很难知道该怎么做的问题。去年秋天，我们决定，我们需要让社群参与进来并获得社群的意见。你提供的总结是社群告诉我们的意见。我要指出的是，对于谁要参加 KSK 轮转，在一定程度上属于自我选择，倾向于倡导 DNSSEC 并有个人资本的人，以及知道在 DNSSEC 中投入了哪些其他资源并想看到轮转实现的人。回想起来，我想我们得到这种情绪并不令人意外，但这就是为什么公众意见非常重要，这样我们可以向更广泛的受众提供关于它的信息，如果人们对此存有悲观的理解，他们可以发表意见。

马克： 我很感激，感谢你的解释。我会继续对此持悲观的看法。我认为我是拥护 DNSSEC 的，所以我无法克服，我会以个人身份对此提出意见。我无法克服自己对第 1 点和第 3 点的悲观理解，对我而言，这里存在着一些任何人都会有的认识差距，认真地提议对根区进行改变而你不知道会产生什么影响。我同意你的看法，我完全相信你对你获得的质量不佳的信号的分析，但是随着时间的推移，你们获得的信号只是诊断信息，你们获得信号只会越来越糟。这是我对情况的描述。我发现在这之后的所有幻灯片都很有吸引力，但是就这张幻灯片中正在讨论中的第 1 点和第 3 点我无法弄清楚。我不知道为什么技术社群中的人会说，在你不知道结果会是什么的时候也要继续实施对根区的改变。谢谢，我将在个人意见中提出这些意见。

发言人（姓名不详）： 我来引述一下我认为可能的另一种理解。这不是我的理解，我只是重复我所听到的内容。这种理解说的是，不对密钥进行轮转可能会导致潜在的不利。即使目前没有密码威胁，它也可能会降低密钥的可信度。无论是对密码本身的威胁，还是对密钥物理操作安全性的威胁。不过，不轮转可能会损害密钥的可信度，如果你认为它不会那么糟糕，人们可以快速修复它，并且你接受一些破损，你就可能会结合所有这些方方面面，认为我们应该对密钥进行轮转。

马克： 我非常理解这种有关声誉的论证，这就是说我们希望进行密钥轮转，因为我们希望人们对 DNSSEC 有信心。我理解其中的声誉部分，另一方面，如果人们猜测错误，我会对这种猜测感到震惊，虽然它实际上比我们认为的要糟糕，但我们必须执行回滚。我们还没有在现实世界中实施过。我认为我们无论如何都会面临声誉问题。这使 ICANN 陷入了困境，我对此非常敏感，但我并不认为 DNS SEC 声誉问题总体来说与 10 月份的未知实施相同。谢谢。

发言人（姓名不详）： 还有其他问题或意见吗？凯西 (Cathy)，我们还有什么来自互联网的问题吗？

发言人（姓名不详）： 没有。

发言人（姓名不详）： 噢，好的。

发言人（姓名不详）： 感谢你的精彩讲解。我的问题是，在尼日利亚，我们发现我们有四家移动网络运营商以及大量的 ISP。我们发现，四家移动网络服务提供商中只有一家在使用 DNSSEC，另外三家移动运营商除了 DNSSEC 之外[听不清]。与其他安全验证系统相比，

DNSSEC 有什么优势？其他[听不清]是否有必要迁移到 DNSSEC？第三个问题是，KSK 轮转之后，使用其他验证系统的网络服务提供商的[听不清]是什么呢？非常感谢。

发言人（姓名不详）： 你能重复一下问题的最后部分吗？

发言人（姓名不详）： 是的，请你重复一下问题的最后一个部分。

发言人（姓名不详）： 我说的是，问题的最后一个部分是，三家移动网络服务提供商没有使用 DNSSEC 验证系统。那么在 KSK 轮转之后他们的[听不清]是什么呢？

发言人（姓名不详）： 抱歉，他们的什么？

发言人（姓名不详）： 他们的[听不清]。会对用户造成什么影响吗？

发言人（姓名不详）： 这个问题很简单，如果你不进行 DNSSEC 验证，那么 KSK 轮转就不会带来任何影响。ICANN 组织的立场是，DNSSEC 验证是

一件好事，所以我们鼓励人们进行 DNSSEC 验证，我很抱歉，现在我不记得你问题的第一部分了。

发言人（姓名不详）： 问题的第一部分是：没有使用 DNSSEC 的运营商迁移到 DNSSEC 之后会有什么优势？

发言人（姓名不详）： ICANN 组织的立场是，你应该进行 DNSSEC 验证，因为如果不进行 DNSSEC 验证你就无法保证你收到的回答是真正在回答你提出的问题，无法保证你收到的回答真正来自你所认为的来源。你没有加密保证，没法确认你所得到的答案真正来自于哪里。DNSSEC 可以让你知道回答是否真正来自于所说的来源，并且自其签署以来没有被修改。现代解析器已经非常聪明，可以避免被欺骗，但最终要获得更高级别的保证，则需要 DNSSEC。没有 DNSSEC，在某种程度上，你就很容易被欺骗，从而相信不正确的回应。

发言人（姓名不详）： 非常感谢，谢谢。

发言人（姓名不详）： 还有其他问题吗？好的，感谢大家参加今天的会议。

[会议记录结束]