ICANN73 | 虚拟社群论坛 — 全体会议：DNS 滥用的演变
2022 年 3 月 9 日星期三 — 大西洋标准时间上午 10:30 至 12:00

布伦达 • 布鲁尔
(BRENDA BREWER)： 准备录音 —

正在录音。

布伦达 • 布鲁尔： 大家好，欢迎参加 ICANN73 全体会议：DNS 滥用的演变。

我是布伦达 • 布鲁尔，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。为了确保 ICANN 多利益相关方模型的参与透明度，请大家使用全名登录 Zoom 会议。也就是连名带姓。如果没有以全名登录，可能会被移出会议。

本场会议将提供阿拉伯语、中文、法语、俄语和西班牙语的同声传译服务。请点击 Zoom 工具栏中的“口译”图标，选择你想要听到的语言。

在本次会议期间，只有用我在聊天室中提供的正确格式在聊天室提交的问题或意见才会被读出来。我会在本次会议的指定时间内大声读出这些问题和意见。在社群会议部分，如果你想发言，请点击 Zoom 工具栏中的“举手”。

发言前，请静音所有设备和通知。另外，请确保你已选择了首选的输入语言。请大家发言时口齿清晰并保持正常语速，以便口译人员准确翻译。

一旦会议主持人叫到你的名字，请取消你的麦克风静音并介绍自己的姓名以便记录。若要查看实时速记，请点击 Zoom 工具栏中的“隐藏字幕”(Closed Caption)。现在让我们欢迎本次会议的主持人，格雷姆 • 邦顿 (Graeme Bunton)。

请开始。

格雷姆 • 邦顿： 谢谢，布伦达。大家上午好、下午好、晚上好。感谢大家参加今天的全体会议：DNS 滥用的演变，恶意注册和被入侵的域名。

我是格雷姆 • 邦顿，是 DNS 滥用研究所的主任。

首先我想说一下，我准备的开场白介绍可能有些长，请大家见谅。这次会议的主题很复杂，我们请来了一些非常优秀的专家组成员，但在正式进入主题之前，我们需要一段非常长的铺垫。所以请大家多多包涵。

第一位发言者马切伊将会对我们这次主题的主旨进行详尽的介绍。为了便于我后面的介绍，我想确认，大家都在同一个页面吧。

我尝试用两句话来解释说明今天的讨论主题。简单来说，我们今天的会议就是探索故意注册以造成危害的域名与被入侵和被黑客攻击的网站所使用的造成危害的域名的缓解流程之间的差异。在前一种情况下，某人是故意利用域名来做坏事，而另一种情况下则不是。我们需要理解我们的生态系统中有着怎么样的复杂性。

在我们进入主旨讨论之前，我想重温一下事关本次会议目标的一些事项，向大家简要概括一下我们准备怎样组织本次会议。

布伦达，请帮我翻到第二张幻灯片。

全体会议目标，这就是我们尝试在短短的 90 分钟会议中达成的目标。我们想要尝试让社群了解，为什么区分恶意注册和被入侵的网站如此重要。我们想稍微谈谈如何做出这种区分，但可能会稍微涉及一些技术问题，所以我们不会太过深入地探讨。

不过我们确实是想入，因为这才是这次对话的干货。我们想让社群了解，在面对恶意注册和域名被入侵这两种情境下可以做些什么，并进行深入讨论。

最后，我们想谈谈潜在的活动，对于这一问题我们可以做什么，由谁来做，以及社群将发挥什么作用。

现在让我们来看看讨论范围。这很重要。长久以来，我作为 ICANN 员工，参加了非常多的全体会议。我认为，主题的特定性和此类会议产生的价值有一定的关联性。所以，我希望大家一起将今天的讨论范围限定在相对较窄的领域内。

这次对话建立在一些设想之上。我们今天之所以在这里讨论，是因为注册管理机构和注册服务机构已经收到了滥用报告。这份报告是如何得到的，不在今天的讨论范围内。我们假设滥用情况已经被证实。假设这些事情真实地在发生。我们不需要讨论它是否已经发生了。所以验证真实性不在讨论范围内。

今天我们将集中讨论恶意软件和网络钓鱼的案例。这也许并不是你们对 DNS 滥用的定义。但可能是大部分人认为的 DNS 滥用，我们今天也不讨论定义。让我再清楚说明一下。我们将不会进行定义性质的讨论，探讨哪些属于 DNS 滥用，哪些不属于。

我们今天需要了解的是恶意注册和域名被入侵的区别。

所以我们这次对话一定要保持专注于这个话题。我们也将记录下不在讨论范围内的评论和提问，看看以后是不是有机会针对这些问题进行探讨。

我将会非常强力地维持秩序，让我们的讨论专注于本次会议的主题。因此我要求大家在提交问题或在聊天中讨论时，应专注于我们的主题，也请理解，我将约束所有人保持专注。

请播放下一张幻灯片。

这是我们今天要进行对话的图示。我们收到了注册服务机构/注册管理机构关于 DNS 滥用的报告。我们需要稍微讨论一下“原因”，为什么我们应该有所区分。所有类型的危害真的都是一种常规的滥用流程导致的吗？如果我们不同意这种说法，那就需要进行区分，我们需要稍微讨论一下如何进行区分。也就是，注册相关的什么属性将能够引领我们做出选择？

在这里我们应该有两个分支。我们应该讨论出一个流程，以应对恶意注册域名，也即涉及故意危害线上安全的域名。还应该有另一个流程，涉及被入侵的网站，我们应该怎么做。

似乎有点乱，不过我认为我们这次对话的实质，真正棘手的是，我们需要弄清楚，作为社群应该如何处理被入侵的网站。随着会议的推进，我们将深入这两个方面进行讨论。

今天我们也邀请了专家组参会。首先我们会邀请马切伊介绍发言，马切伊是格勒诺布尔大学的教授，我想你应该是法国人，有谁能给我们一些资料，让我们了解一下具体情况。发言将持续大约 15 分钟的时间。

然后我们会直接进入专家组讨论。我们的专家组中有很多著名人士。非常感谢你们参与讨论。我们有来自知识产权选区 (IPC) 的洛里 • 舒尔曼 (Lori Schulman)；来自政府咨询委员会 (GAC) 公共安全工作组的克里斯 • 路易斯-埃文斯 (Chris Lewis-Evans)；来自注册管理机构的艾伦 • 伍兹 (Alan Woods)；来自注册服务机构的雷格 • 利维 (Reg Levy)；以及来自安全与稳定咨询委员会 (SSAC) 的罗德 • 拉斯穆森 (Rod Rasmussen)。我们将要深入探讨这些主题。

大致分为两个部分。首先，我们将进行介绍，然后稍微探讨一下恶意注册，再然后详细讨论被入侵的网站。

我们将省出大量的时间，用于最后的问答环节。在整个对话期间，都将开放问答功能，我鼓励大家积极使用，但一定要注意，我们必须要专注于今天的主题。

如果你的提问没有得到回答，请记得，我们会记录下来并在以后合适的机会展开讨论，所以如果因为你的提问与今天的主题不符而没有得到回答，也请不要生气。

这就是我想介绍的了，稍微有点长，不过我希望可以给大家一些预期，明确我们的目标以及讨论范围，现在是时候进行深入探讨了。

现在我准备将话筒交给马切伊，由他来谈谈，面对现在的恶意注册和被入侵的域名，“目前正在发生什么”。

马切伊，请发言。

马切伊 • 科尔钦斯基 (MACIEJ KORCZYNSKI)： 谢谢格雷姆的开场介绍。

大家好。今天我想谈谈被入侵的域名和恶意注册的域名。它将主要基于受损注册域名与恶意注册域名的分类 (COMAR) 项目，这是由法国互联网域名与合作协会 (AFNIC) 和 SIDN 资助的一个研究项目，它们俩分别是 .FR 和 .NL 域名的注册服务机构运营商，而在技术方面，则主要是基于由欧盟委员会委托的关于 DNS 滥用方面的研究。

请播放下一张幻灯片。

在最上面我们可以看到一个被 Phish Tank 加入黑名单的 URL，而下面可以看到一个恶意网站，恶意网站的截图。我们今天要解答的问题是域名是否被恶意注册。请播放下一张幻灯片。

为了找到问题的答案，我们需要稍微做一下调查。当我们访问注册的域名时，可以看到那里并没有什么有意义的内容，而当我们查看 WHOIS 信息时，会发现该 URL 是在被加入黑名单的两天前注册的。

请播放下一张幻灯片。

这就为我们提供了强有力的证据，证明该域名是被恶意注册的，并且可能被滥用，以服务于非法和滥用的内容、网络钓鱼凭证和商标侵权。

这其中的隐含意义是什么？从技术角度来看，什么样的中介能够缓解滥用？应该是 DNS 服务运营商，例如注册服务机构，甚至 TLD 注册管理机构，还有托管服务提供商。为什么这很重要？因为如果我们仅仅只是中止域名而不是恶意托管服务，那么攻击者就可以很轻松地注册另一个域名并指向恶意托管。另一方面，如果我们仅仅只是中止托管服务而不封锁域名，那么

攻击者就可以在其他攻击中，在其他网络钓鱼活动中再次使用该域名。

所以为了增加攻击者的域名滥用壁垒和经济成本，从技术角度而言，缓解措施应该同时施用于 DNS 和托管服务层级。

请播放下一张幻灯片。

让我们来看看另一个案例。我们这里有另一个 URL，一个恶意 URL，我记得已经被反网络钓鱼工作组加入了黑名单。下面我们可以看到恶意网页的截图。同样的问题又来了，该域名是被恶意注册的吗？

请播放下一张幻灯片。

于是我们访问了注册的域名，这个网站显示着合法的内容，而且内容本身也与该域名有所关联。让我们来看一看 WHOIS 信息，该域名在 2014 年被注册，所以该域名本身极有可能是合法的。

另外，让我们看看该恶意 URL，我们发现有包含有 wp 字样，这表明实际上该网站被黑客利用脆弱的 Word Press 安装入侵。

请播放下一张幻灯片。

所以该域名是合法的，但网站被入侵和滥用，以服务于非法和滥用的内容、网络钓鱼凭证和商标侵权。

那么从技术角度而言，这又隐含了什么意义？

所以通常来说不应该由注册服务机构或 TLD 注册管理机构来封锁域名，因为那样会对注册服务机构、域名背后的商家以及网站的合法访问者造成附带损害。缓解措施应当施用于服务托管层面，由托管服务提供商或者网站的拥有者或管理员执行。这里有两件事要做。首先，清理恶意内容，并为易受攻击的漏洞和 Word Press 安装打上补丁。

那么现在，应该由谁来做？如果托管服务受管理，则应该是管理服务提供商，例如在共享托管平台上，托管平台控制着所有的软件，包括易受攻击的软件，如果托管服务不受管理，则应该是 web 管理员，这种情况下管理员控制着易受攻击的软件。

请播放下一张幻灯片。

合法的域名如何被滥用？通过我们的分析发现，域名主要是在网站层级被滥用。也就是易受攻击的软件被黑客利用，例如内容和高级系统。有时也发生在 DNS 层级。这里的例子是域名阴影，攻击者将会首先尝试通过网络钓鱼获得注册服务机构、

注册人的凭证，从而侵入他们的注册面板。一旦他们登入注册面板，就可以添加子域，然后利用子域进行网络钓鱼攻击。请播放下一张幻灯片。

那么现在有什么方法可以将合法但被入侵的域名与恶意注册的域名区分开来？

有两种方法。第一个方法基于启发法，在行业报告中常常会用到这种方法。其中一种启发法就是看域名的年龄。正如之前的示例，观察域名的注册时间和被列入黑名单的时间、域名是否是批量注册，以及域名注册的模式。举例来说，对于网络钓鱼攻击，目标服务往往会出现拼写错误的品牌名，例如 PayPal。

另一类方法是机器学习法。例如，由 AFNIC 和 SIDN 资助，格勒诺布尔大学开发的 COMAR 项目，它是一种完全自动化的方案，理念是根据所收集的与网站托管服务、与 URL 结构相关的数据、域名的特定 QR 等等，我们提取出了 38 项特征。这个项目基于建模系统完全自动化，目前显示出高达 97% 的准确率。

请播放下一张幻灯片。

那么这两种类型的滥用，即被入侵的域名与恶意注册的域名之间的关系是什么？请翻到下一张幻灯片。

这里显示了每种滥用类型的分布，被入侵的域名为蓝色，恶意注册的域名为红色。通常来说，要控制垃圾邮件和购物网站，攻击者需要控制 DNS。但是，对于网络钓鱼和恶意软件，则不需要。只需要使用恶意注册的域名或者入侵网站和免费服务，就能实施攻击。

大约 25% 的网络钓鱼域名和 41% 的恶意软件分发的域名是由合法用户注册的，但大部分都属于网站层级的入侵。

请播放下一张幻灯片。

不同类型的 TLD 有这样的变化？2021 年的下半年，我们观察到，对于新的新通用顶级域 (gTLD)，几乎 98% 的域名都被标记为恶意注册。请看左边的欧盟国家和地区顶级域 (ccTLD)，42% 的域名被标记为网站被入侵。那么可能的原因是什么？我们猜测，在欧盟和国家和地区顶级域，投机性的注册较少，功能完善、提供有意义的内容的网站较多，这也就意味着它们部署了可能会被网络犯罪分子大规模攻击和利用的各种不同软件。

请播放下一张幻灯片。

不同的 TLD 有这样的变化。

抱歉，可能连接断开了。我看不到演示文稿。

格雷姆 • 邦顿： 现在好了，我们能够听到你，马切伊。

马切伊 • 科尔钦斯基： 好的。但是我看不到演示文稿。

格雷姆 • 邦顿： 现在是在第 13 张幻灯片。

马切伊 • 科尔钦斯基： 好的。我切换回我的本地版本。好的。

这里我们看到不同的 TLD 中，域名的总数，被滥用的域名数，尤其是恶意注册的数量和被入侵的数量，在最后一栏，我们可以看到恶意注册的数量相对于所有 TLD 被滥用域名数量的百分比。请播放下一张幻灯片。

这里可以看到，在某些 TLD 中，恶意注册的域名占比几乎为 100%。

顺带提一句，.TK 和 .ML 域名是 Freenom 免费提供给其用户使用的，这对于网络钓鱼攻击者来说，是个非常有吸引力的后门。

请播放下一张幻灯片。

另一方面，我们还看到这样的 TLD 例如 .Br，恶意注册的域名仅占 34%。这可能是由多个因素造成的。我想请大家注意，那样的结果需要谨慎对待，因为它们本身具有分类器限制和黑名单限制。所以它们无法代表整个网络。

为什么会那样？因为某些黑名单提供商可能会通过识别特定的关键字等方式，聚焦于恶意注册的域名。

所以我还想说的是，我们在黑名单中看到的域名可能与 TLD 注册管理机构分析网络攻击受害者的投诉时所看到的域名不同，因为那些黑名单可能不具备足够的代表性。

最后我想说的是，随着时间的推移，我们看到，同样的 TLD 中也发生了很大的变化，例如 .INFO 或 .COM，每个月都有变化。这究竟是什么原因呢？一个可能的理由是，某位经销商为它的大客户提供了易受攻击的域名。在这种情况下，我们将看到恶意注册的域名数占被滥用域名总数的百分比会有所增加。举例来说，随着时间的推移，我们看到一些漏洞被发现，例如内容

管理系统中的漏洞，对成千上万的域名造成了影响。而这对于攻击者来说，也犹如唾手可得的猎物。他们可能会实施大规模攻击。然后在这样的情况下，我们将会在很短的时间内看到，恶意注册的域名数在域名总数中的占比下降。

请播放下一张幻灯片。

非常感谢大家的关注。希望这有助于开启我们的讨论。谢谢！

格雷姆 • 邦顿： 谢谢，马切伊。在你发言的过程中，还顺带回答了很多大家提出的问题，非常感谢。

不过在聊天框中还有一些问题，马切伊，围绕的是我们是否能通过机器学习实现这类区分？现在有算法可以做到吗，准确性如何？我觉得我们不需要深入了解“原理”，但如果你用两三分钟时间介绍一下域名或网站的各种属性，以及工具是如何自动尝试完成这项工作的，又或者你知道在技术不成熟的情况下人们可以尝试使用什么工具，那应该会很有帮助。你可以介绍一下吗？

马切伊 • 科尔钦斯基： 当然可以。对于第一个问题，我们在 COMAR 分类器中对功能的重要性进行过分析。

所以正如我在发言过程中所提到的，COMAR 分类器就是全自动的机器学习算法。基于内容的的功能是非常有用的。例如，如果我们检测到网站使用了非常多不同的技术来构建，那么这表示该网站已经被入侵了。

如果我们看到明确的关键字，如“PayPal”，不仅仅是品牌名字，还包括非常具体的关键字，我们也会对这类关键字进行分析验证。这会指示网站是否是恶意注册的。

要知道，有些东西可以被分类器取回，例如所使用的技术的数量，而这是人工很难做到的。

另一方面，如果我们想要通过人工完成区分，那么也可以借助一些东西，比如我们在示例中看到的，注册的时间和被列入黑名单的时间。如果两者非常接近，就是域名被恶意注册的强证。

如果在注册的域名上，或者说注册的域名下的网络钓鱼网站上没有什么有意义的内容，那么也表明该域名是被恶意注册的。

这两个例子对于人工和机器而言，都是非常好的示例，可以通过机器学习来检测此类情况。

格雷姆 • 邦顿： 很好。谢谢，马切伊。聊天框中还有一些内容。我没法完全跟进，因为内容有点多。所以如果你们有想要获得解答的问题，再次强调，是与主题有关的问题，请使用问答功能，这样我们会尝试记录下来。

还有好多提问是围绕“如何”进行这项检测的。你们可以去看看 DNSAI 最近编写的一项最佳实践。

我相信有人会找到链接并发在聊天框里。谢谢。

我也在周一的技术日上制作了一个演示文稿，其中罗列了此类解决方案，提供了一个展示“如何”完成此项工作的框架。

我想我们接下来应该更进一步，讨论“如何”之外的其他事项了。很清楚的是，在确定这些注册是否为恶意为之时，无论是技术方法还是人工方法，都牵涉非常多的利益关系。我想接下来应该进入到“为什么”以及“是什么”的讨论了。

这将是我向专家组提出的第一个问题。请专家组注意。

这是一个门控问题：我们应该全面这样做吗？如果我们把缓解流程区分开来，这样做有意义吗？我们需要区分恶意与否或者被入侵与否吗？要知道，我们应该对所有情况都采用同样的方

法吗，也就是一个通用的防止滥用方法，或是应该采用不同的流程？

我也想知道，是否有人不同意我们的整个前提。我们以同样方式对待滥用吗？

让我们从那里开始，看看是否有专家组成员想要发言。

我会请你发言的。雷格，请发言。

雷格 • 利维 (REG LEVY)： 好的。是的。我任务区分是绝对有必要的。我们有许多使用商业网站创建器的客户需要常规的更新。如果他们不进行更新，则通常很容易被攻击和入侵。所以我们要联系注册人，与他们讨论事实情况，十年前他们就需要在域名方面做一些事情，甚至自他们设立网站起的五年中，他们压根没有想过。他们只是使用电子邮件，并猜测人们可以访问网站，看到他们的信息，并且能够联系到他们。我们需要确保他们的业务不受影响，因为针对域名的攻击确实存在。

格雷姆 • 邦顿： 谢谢，雷格。

接下来是艾伦发言，然后依次是克里斯和洛里。我的意思是，我们不需要在“为什么”方面进行太过深入的讨论。让我们先听听几位的发言。然后再继续。

有请艾伦。

艾伦 • 伍兹 (ALAN WOODS)： 非常感谢。我是艾伦 • 伍兹。

是的，我认为这项区分非常重要。我知道，我们进行区分的理由已经被提出来好多年了。但是从注册管理运行机构的角度来看，当我们针对域名采取行动时，会造成很多连带的损害。因此，我们并不想牺牲其他人，也就是被入侵的注册人。

我认为，我们需要非常清晰，如果我们要采取行动，那就应该考虑到（恶意注册和被入侵的域名）区别。我曾经提到“细微差别”，但这两种类型的受害者之间也有差别。

格雷姆 • 邦顿： 是的。谢谢艾伦。

克里斯。

克里斯 • 路易斯-埃文斯
(CHRIS LEWIS-EVANS)： 谢谢格雷姆。我是克里斯 • 路易斯-埃文斯。

我同意这种说法，我们应该区分对待这两种情况。正如艾伦所说，我们面临着两种不同类型的损害。对于恶意注册的域名，肯定会造成主要损害。而对于被入侵的域名，除了主要损害之外，还会造成连带损害。

对于被入侵的情况，也有两种类型的受害者：主要的受害者以及被连带损害影响的受害者。所以我们需要面对这两种类型，为他们提供足够的帮助。

格雷姆 • 邦顿： 谢谢，克里斯。

洛里，请发言。

洛里 • 舒尔曼
(LORI SCHULMAN)： 好的。我要说的是，IPC 也同意，我们绝对有必要进行区分。至少在前端，区分恶意注册的域名和被入侵的域名，事关我们能否针对特定问题快速做出响应，所以这种区分非常重要。

但同时，我也不想漏掉在这种区分下的实际受害者，也就是最终用户，遭受网络钓鱼攻击、恶意软件攻击的最终用户。

当然还有小型商业用户，他们的业务和商誉都可能潜在地遭到损害。我认为我们不应当臆测在网站上运营商业活动或者运营实体机构的注册人一定不愿意出于保护他们的客户或商誉的目的暂停网站活动一段时间。

格雷姆 • 邦顿： 谢谢洛里。

我想要说的是，至少在我们的专家组中，没人不同意这个问题，我们确实需要进行区分。那样很好。

但也增加了复杂度。所以现在我们需要稍微深入讨论那样做意味着什么。我之前说过，问答功能中积累了一些提问，我想也许我们应该在尝试解答这些问题后再继续，以便保持相关度。我会挑选一些问题，分配给讨论组成员们。让我们试一下。

来自格雷格 • 沙坦 (Greg Shatan) 的问题，我想应该分配给马切伊回答。他的问题是：邮件服务器层级的滥用与你们提出的方案的适用度如何？

我认为邮件服务器层级的滥用相当有趣。我对这方面了解得不太多。

马切伊，你对此有什么想法吗？

马切伊 • 科尔钦斯基： 邮件服务器？

格雷姆 • 邦顿： 我想格雷格问题涉及通过电子邮件实施的网络钓鱼和恶意软件攻击。

马切伊 • 科尔钦斯基： 是否有可能让提出问题的人简单说明一下？

也许这样更便于使问题清晰。

格雷姆 • 邦顿： 我有点担心用这种方法开实时语音的效果如何。

也许格雷格可以在聊天框中稍微阐述一下问题，然后我们再来回答。

马切伊 • 科尔钦斯基： 谢谢！

格雷姆 • 邦顿： 看看他是否能解释说明一下。

马切伊 • 科尔钦斯基： 非常感谢。

格雷姆 • 邦顿： 那么在我们继续之前，还有什么可以回答的。天呐，还有好多。请见谅，我会尝试挑选出一些相关性比较高的问题。

另一个提给马切伊的问题来自于莎曼内。她想知道，COMAR 中使用的 ML 方法和功能是否也包括你在第一个方法中指出的启发法。如果是的话，是否有什么示例？

马切伊 • 科尔钦斯基： 谢谢你的问题。是的，我们在这些方法中囊括了启发法使用的几乎全部功能，批量注册除外。这是我们唯一没有囊括的功能。原因是，我想说，有两个原因。一个主要原因是，COMAR 方法只应根据收集到的数据来区分恶意注册与网站被入侵，并且只能关联一个具体案例，而不能从其他恶意注册的域名去获取信息。

不过除此之外，所有的启发法都会在 COMAR 系统中完全自动执行。

格雷姆 • 邦顿： 谢谢，马切伊。

这里还有一个问题提给你，来自迈克尔 • 派拉格 (Michael Palage)，他对你提到的欧洲 ccTLD 中被入侵的域名占据的高比例感兴趣，这是否应该归因于越来越多的 ccTLD 在执行身份核对？与使用欺诈性或伪造的注册人数据注册域名相比，恶意人士入侵域名/网站更容易吗？

马切伊 • 科尔钦斯基： 如果我理解正确的话，这个问题是说，为什么我们会看到欧洲 ccTLD 中，恶意注册量较少，而被入侵的网站更多。对吗？

这个问题的答案在我的演示文稿中尝试进行了一些探讨。但是我们也只能猜测，因为我们还没有进行任何计算。

但我要说的是，在欧盟 ccTLD 中，我们看到的停放域名较少，也就是投机性的域名并不太多，正如我之前提到的那样。域名的背后是网站。如果是网站，那么网站的用户也会照看它们。他们会部署不同的软件。因为我们看到网站上有许多不同的软件，而其中有些软件则很容易被网络攻击者利用。

我想问题的第二部分是，为什么我们看到的恶意注册的域名较少。这也纯粹是推测。也许 ccTLD 有许多方案来阻止恶意注册。比如，在欧盟 ccTLD，有一个类似 Premadoma 的系统，会在域名注册时检测它是否为恶意注册。或者有其他 ccTLD 能够主动对抗和阻止恶意注册，例如 SIDN AFNIC。

不过这只是从我的经验和研究，以及我在 ccTLD 看到的情况而言的。这并不意味着，其他 ccTLD 或其他 ccTLD 小组不会部署这些防范方法。

格雷姆 • 邦顿： 谢谢，马切伊。

天呐，我们收到了很多问题，聊天框里也内容繁多。我们将尽量掌控，不要偏题。

专家组成员们，如果你们想要回答问题，无论是实时发言还是通过问答功能回复，请尽管行动。

我认为也许现在，我们应该前进到图表的左侧部分，开始讨论针对恶意注册应该设立什么样的流程，或者要有什么样的考量。再次确定一下，我们都在同一个出发页面吧，我们确定应当进行区分。我们刚刚稍微探讨了一下这样的决定是如何做出的。我们也了解了域名的一些属性。可能是 ML。可能是执行的人。现在我们需要探讨的是下一步要做什么。

在注册管理机构和注册服务机构层面，我们的选择并不多，但也许我们应该稍微探索一下。

这次我将话筒交给罗德。罗德，当注册管理机构或注册服务机构遭遇恶意注册性质的 DNS 滥用时，他们应该采取怎样的行动。

你有什么想法吗？

罗德 • 拉斯穆森： 好的，谢谢。我叫罗德 • 拉斯穆森，

一旦你确定了，无论你是使用什么方法确定的，都把它放在一边，因为我们并不聚焦于此。我们说，现在已经确定了这是恶意注册，那么我能做什么？

作为注册服务机构/注册管理机构，你的选择真的很少。我们的主要手段是一样的，那就是将域名从全球 DNS 中移除。

实际上你可以通过几种方式来完成移除。你可以立即当场删除它，也就是最基本的，删除这次注册。如果恶意注册已经完成，比如在前几天已经注册完成了，那么你实际上可以获得一些财务方面的补偿。换句话说，你能把钱要回来。这是一项优势，但这么做也通常存在劣势，因为最初注册域名的人可以通过相同的注册服务机构或者在别的地方再次注册，只需要重新启动他们的计划即可，甚至假设你 — 同时也有人在消除恶意内容，但要知道的是，他们有非常多被入侵的网站可以重新建立恶意内容。所以优势和劣势并存。

你可以中止域名。换句话说，不删除它，但是将其置于中止状态。那会将它从 DNS 中移除，但在整个注册的生命周期内，它都将处于中止状态。然后，你可以作为注册服务机构或注册管理机构对它们进行管理。

然后你也可以采用其他有效的缓解措施。多年以来，反网络钓鱼工作组提供了网络钓鱼网站登陆页，所以如果遭遇网络钓鱼攻击，你可以将其重新定向，你可以更改 DNS，将其指向网络钓鱼登陆页。其他人已经做过类似的事情了。如果遇到的是恶意软件，那么你可以创建一个所谓的“排水口”，让你能够通知受害者，他们的机器已经被入侵。这已经通过很多不同途径完成了，有的是直接由提供商完成，有的则是通过网络安全公司、立法机构等等。所以其实你可以积极主动地尝试让各种恶意软件的受害者知道他们的机器已经被感染。为了这么做，你可能需要将域名传输给其他实体，或者从注册服务机构到注册人代表。例如，FBI 已经查封了一些域名并进行了传输。微软公司也做过多次这样的操作。

你也可以利用 Last Resort 的注册服务机构，它已经设置好接收恶意软件注册的命令与控制型域名，然后将数据自动提供给受害者。所有你有几个不同的选择，但必须要确保先准备好相关流程和法律文书。

最后我想说的是，一旦你确定了恶意注册的域名，最好可以看看是否有其他域名与之相关联，或者被同样的注册人或注册人帐户所使用。查看该帐户的情况，这非常重要，我想雷格或其他人可能会谈得更深入一些，这是要了解该帐户是否是被同样的恶意行动者所设置的，或者是被入侵并添加了域名的，因为它们也可能是网络钓鱼或其他凭证盗窃攻击的受害者。

然后另一件要做的事情就是，找出这一系列帐户的创建模式，它们可能是在不同的别名下创建的，从而发现更宽泛的域名滥用情况，也许注册人帐户能够引导我们发现大规模的攻击活动，因为有些攻击者非常精于隐藏自己，从而不被勤奋的注册服务机构拒于门外。

以上就是我的一些想法。

格雷姆 • 邦顿： 谢谢，罗德。非常好。有很多内容。

我简要复述一下：注册服务机构有三种或更多种方式，或者说比注册管理机构更多，尽管注册管理机构也可以参与进来，不过你可以删除，可能不是最好的方式，你可以中止，或者可以指向或重新定位。选择这三种方式都有各自的理由。然后你应该查看帐户，你应该查看该帐户是否符合不同的模式。我想所有这些内容都对意图缓解滥用情况的人非常有用。

我想知道我们专家组的雷格或艾伦对此有什么想法。他们会经常运用这些方法吗？如果会，原因是什么？如果不会，原因又是什么？

不过在你们思考的同时，让我们先有请洛里。

洛里 • 舒尔曼： 谢谢！刚刚罗德的发言中提到，找出滥用的模式，从而找出更宽泛的示例，对此我有个问题。如今我们面临的隐私法规和政策越来越收紧，那么这样的研究是仅限于特定的注册服务机构吗，或者在注册管理机构比注册服务机构更适合的情况下，由注册管理机构对大范围的注册服务机构进行此项调查？

格雷姆 • 邦顿： 是可以的。谢谢，洛里。

罗德？

罗德 • 拉斯穆森： 好的，我来回应一下这个问题。两种情况都可以（笑声）。注册服务机构有一项独特的能力，能够看到从公众视角看不到的信息，例如联系信息等等，当采用类似启发法等方式进行调查时，这是一项非常有价值的资产，马切伊刚才也谈到了。他们

能看到注册来自于哪里，使用了是什么信用卡等等此类信息。所以从内部来讲，他们有很多数据可以用来调查。

从外部来讲，注册管理机构能够很好地了解到是否存在支持我们所谓的域名生成算法的模式。那些是恶意软件使用的，它们会预先确定一系列要注册的域名，从而为恶意软件家族提供命令与控制。如果你看到不同的注册服务机构都有一系列这样的注册，那么就知道这是一种模式。

他们还可以观察类似 DNS 托管服务的事情，以及域名在互联网上的实际配置方式。如果你查看它们针对特定 DNS 服务器、域名服务器或者最终托管 IP 地址而设置的方式，通常就可以检测到此类事情，至少会发现可疑之处。你不妨与注册服务机构深入谈谈并让他们查看可疑帐户，看看是否是非法的。

格雷姆 • 邦顿： 谢谢，罗德。

只是一个想法，对于克里斯。如果你，如果不是很着急的话，我想先请雷格和艾伦发言，然后再请你发言。不过在我们从这个主题继续进入到被入侵的讨论之前，我想知道，从执法的角度来看，对于恶意注册，你们是更愿意中断恶意注册，还是会更多地参与到调查中，从而通过流程收获更多信息。

雷格和艾伦，请简要发言。然后由克里斯发言。然后我们将尝试进入被入侵相关的讨论，再然后进行更多的问答。

有请雷格。

雷格 • 利维： 谢谢你，格雷姆。我是来自 Tucows 的雷格 • 利维。我们属于批发注册服务机构，所以我们处理这种情况的方式可能与直接面对注册人的注册服务机构稍有不同。

我们主要与分销商合作，并依据分销商的情况找出模式。所以当大量的滥用情况来自于某个特定分销商时，我们会联系他们说：“嘿，我们是处理 DNS 滥用的专家，有什么可以帮到你吗？”通常我们会在那样的基础上解决问题。

尽管如此，我们也还有一个内部分销商，当我们看到大量恶意注册域名来自于他们时，就可以直接针对可以的注册人采取行动，只要它是可辨别身份的实体。

聊天框中已经提到过，网络欺诈攻击者通常不会使用他们自己的名字或者相同的名字来大量注册域名。所以寻找类似那样的模式并不总是有效果。

我想最初的问题应该是，我们是否会在域名被注册时进行查看，以便确定它是否为恶意注册或者是否被入侵？是的，我们一定会这么做。但不幸的是，很多 AI 缺少信息，或者创造了范围太过广泛的关停情况，正如我们在聊天中提到的那样。所以我们需要大量的人工检查，看看 AI 实际代表着什么。

实际上，我最喜欢的一个案例与域名生成算法有关。有个笨蛋使用域名生成算法 (DGA) 设法注册了一个看似由随机字母组成的字符串，那好像是在中美洲的一支很小的女子足球队的长缩写。所以（笑声）我们与执法机构和注册管理机构合作，允许他们进行注册。

这是又一个例证，这些基于计算机的算法撒的网非常大。抱歉。

格雷姆 • 邦顿： 谢谢雷格，很有趣的事情。

有请艾伦，然后是克里斯。请尽量简短发言，以便我们可以继续会议。谢谢。

艾伦 • 伍兹： 好的。我会很快讲完。追查注册服务机构是很棒的，因为这就是注册管理机构在这种特定情况下应该采用的方式。所以我要

说的跟雷格刚刚说的一样，只是更上一层。她会与她的分销商交流，或者与她的注册人交流，而在第一个示例中，我则会首先与我的注册服务机构交流。我认为站在注册管理机构的角度，这很重要，当我处于那个位置时，我将查看那些指标，我的后端平台 TDNS 将为我做这项工作，然后再根据证据升级给我的注册服务机构，这样他们就能与他们的注册人展开更具针对性的对话。

我认为目前我们有点跑题，进入了关于检测的交流，而这是我们暂时不想涉及的，因为我们将会讨论被入侵的情况，以及我们会做什么和如何做。我认为那是那个主题中很重要的方面。

我还想说的是，站在注册管理机构的角度也非常重要。我想稍微回到刚刚洛里说的，关于小型商业用户更愿意或者更不介意业务暂时停滞。我认为大部分小型商业用户都不会同意这种说法。我们需要明确一点，这是一种具有均衡性的损害。这种损害是否会伤及注册人或最终用户更甚？如果我们能够在均衡性的基础上工作，而不是发表更大或更广泛的声明，我认为这肯定是关于相称性的，我们需要在这里讨论。

格雷姆 • 邦顿： 谢谢艾伦。那将是我们下一阶段讨论的一个很好的话题，在听完克里斯发言之后，我们将回到关于损害的平衡性的讨论。

克里斯 • 路易斯-埃文斯： 好的，谢谢。我是克里斯 • 路易斯-埃文斯。

我们继续讨论恶意注册的域名，格雷姆，我在考虑你提给我的问题，是的，今天晚些时候我们将会讨论恶意软件和网络钓鱼，所以大体上，我们将会有一些调查形式。任何人都不会意外，通常他们不会只注册一个域名。

所以域名将会被调查，我们也会跟注册管理机构、注册服务机构或者托管服务提供商合作识别更多的域名，从而将被动工作转变为主动工作，防止造成更多的受害者和进一步的伤害。所以这就是执法机构一直想要做的事情，那就是改变事态，防止伤害。

谢谢！

格雷姆 • 邦顿： 谢谢，克里斯。

好的。我们还剩 35 分钟的时间，我们看到排队中的提问很多，聊天框中的讨论也热火朝天。非常感谢大家的热情参与。我认为，我们现在完成了简单的工作，也就是我们确定了，想要进行这种区分。我们也简单讨论了如何区分。罗德提到了在面对恶意注册时的一些很棒的应对方式。现在我们转向另一面，我认为是一种更为复杂的 DNS 滥用案例，也就是被入侵

网站上的恶意软件和网络钓鱼危害。网站本身是良性的。可能是小型商户的网站，也可能是某人的博客。而这是我们将要进行的讨论。

在这种情况下，有什么流程可以让我们做些什么。人们通常所做的危害平衡是什么？

我将再次向雷格和艾伦提出启发性的问题，那就是，如果你们确定某个网站正服务于网络钓鱼或者恶意软件，参与到了 DNS 滥用中，那么是否存在某种情况会让你们把它下线？也就是说你们会中止被入侵网站的域名。

艾伦？

艾伦 • 伍兹： 谢谢！这几乎就是我的专业，事关损害的不均性。这是个有趣的问题，我想，作为注册管理机构，我们必须要有一个非常非常直击要害的手段，那就是删除网站和域名上的一切内容，以及与该域名相关的所有电子邮件。所以为了让注册管理机构真正掌握话语权，你知道吗？在这个案例中，我没有从注册服务机构获得任何回应，也没有从注册人处获得任何回应，而客观存在的严重危害仍在发生。我的意思是，一定要有一个时间点，让我们可以删除一切，但是事关危害的均衡性。我们讨论的是 — 抱歉，我会说慢一点，方便翻译。我有点激动了。

要知道，我们讨论的是对人们的生活造成危害的事情。我们讨论的是诸如儿童性虐待材料等一些非常令人不适和有争议的内容。我们需要非常清楚的是，在任何可能的情况下，注册管理机构都不应当成为取缔域名的机构，但在必要的情况下，我们有这个选择。

格雷姆 • 邦顿： 谢谢，艾伦。

雷格 • 利维： 接着说 —

格雷姆 • 邦顿： 请继续，雷格。

雷格 • 利维： 说到这方面，我们倾向于使用中止作为对待被入侵域名的终极手段。我们会直接联系分销商和注册人，跟他们说：“现在出了点问题。你们能修复吗？”然后根据他们的回复或者不回复，我们会逐个重置各条记录，从而关闭邮件，如果入侵发生在那里的话。如果入侵发生在域名服务器，我们可以重置域名服务器。

有时候这会提醒人们回复说：“嘿，我没留意到你发的电子邮件需要我进行回复，你能将我的（听不清）上线，然后我来修

复吗？”这是事情的另一方面，有时我们需要允许域名解析，以便他们登录网站并修复问题。

所以中止域名虽然能够摆脱恶意使用，但也会阻止其他用途，也没法缓解滥用。

格雷姆 • 邦顿： 谢谢雷格，谢谢艾伦。

我想请问洛里、罗德、克里斯，是否有你们认为应该包含进注册服务机构经常参与的危害均衡性测试中，但却未得到充分代表的信息，或者说，在人们思考如何处理涉及 DNS 滥用的被入侵网站时，应该加以考虑的信息。

洛里 • 舒尔曼： 是的，格雷姆。如果你不介意的话，我想首先发言，针对聊天框里的讨论。因为我在聊天框里阐述了一个观点，扩大了讨论的范围。但这回到了雷格阐述的内容，我也同意她的阐述，当你查看被入侵的域名时，你并不一定总是在查看一组事实。这才是我想在聊天框中表达的观点，但现在我感觉有点被过度解读了，对吗？

当你查看被入侵的域名时，关于你要做什么，你要什么时候做，你要怎么做，因为这涉及到 — 可能是一种（听不清）模

式，一个正在运营的网站，提供某项服务或其他权益，如果我们中止域名，这种权益就会消失。而这可能会影响某人的收入。这些我很清楚。

不过我想表达的观点是，这也是罗德和艾伦指出的，我们讨论的事情与网络钓鱼和恶意软件有关，所以要视情况而定。这个站点被入侵了吗，它现在在提供色情内容？我甚至准备说，甚至准备举例说儿童色情内容，这样我们就不会有任何争议。你们知道，我们社群所确定的案例肯定不是极端案例。我们将会看到 CSAM，这是我的亲身经历，有个网站被入侵了，然后开始在网站上看到了 CSAM。重申一下，我将更多地以小型商家为例，而不是大型商家，因为大型商家在应对某些事情时，往往有着不同的决策方式。而利益相关的小型商家可能会说：“我们不需要与这个域名关联的 CSAM。我们推销这个域名。我们在这个域名上有 SCO。”现在必须停下来。我们得暂停一下。我们得重置。我的观点是，你不可能针对各种被入侵的域名采用通用的解决方案。我想最好可以 — 抱歉，我讲话太快了。我马上慢下来。抱歉。那是因为受到美国东海岸的熏陶。抱歉。

我会慢慢说，我想说的是，我们需要有所区别的决策树来处理各种被入侵的域名。我们不能假设商家可能会或可能不会做什么，除非情况非常极端，这一点与艾伦的看法一致。

但我们不能忽视他们，一定不应忽视，我很赞赏 Tucows 的做法，它与分销商的沟通非常好，让分销商知道正在发生什么事情。

我认为平衡问题的重要组成部分是我们有时间根据危害的程度和发生地点进行考虑，然后我们可能会顾及注册人，他们可能会处于最佳利益考虑将域名中止以便进行重置，这样他们围绕域名开展营销和宣传的效果就不会被“稀释”，这是个商标方面的专有名词。但在这个意义上，一个原本良好、受人尊敬的商业实体很可能会被我们在实践中看到的各种入侵而毁掉。

希望我说得足够慢了。

格雷姆 • 邦顿： 谢谢洛里的发言。

有请克里斯，然后是艾伦。然后我这里有个提给专家组的问题。

克里斯。

克里斯 • 路易斯-埃文斯： 好，谢谢。就我而言，我认为在恶意域名方面，注册管理机构和注册服务机构利益相关方团体所做的工作非常好，我们关于滥用通知的证据标准的建议被采纳了。

对于被入侵的域名，这部分工作还没有完成。我认为要让注册管理机构和注册服务机构行动起来，需要有一定的证据标准，就被入侵的域名进行更详尽的解释说明。

你们知道，作为滥用情况的报告方，我们可以说，我们已经联系了托管服务公司，我们已经联系了注册服务机构，但为什么没有任何行动？无论时间多长，都有待讨论，并再次归结为造成的伤害。

聚焦于我们的限定讨论范围，我们讨论的是恶意软件，但你们知道，目前还有很大一部分勒索软件在肆虐。被勒索软件找上门一次，就可能导致业务终结，许多人失业。

因此我们能够在适当的证据标准下阐明这一点，我们最近针对 Amotech 进行了一次大规模行动，后者对企业和个人造成了巨大的伤害。我们能够清楚地说明这一点，并表示我们已经联系了注册人，联系了托管服务提供商，但什么都没有发生，因此我们现在联系你、注册服务机构或注册管理机构寻求中止域名，这样就走完了决策流程。

我们也了解，这随后可能会转向讨论，你知道吗？这是你要求我们中止域名的一家大型跨国公司。影响可能会非常大。实际上，这种网络钓鱼攻击只以少数人为目标。它的目标市场很小众，但影响却很大。我们可以给注册人 48 小时的时间响应，然后我们增强请求。

我认为关于被入侵的域名，可以交流讨论的内容非常多。它确实能在主要方面和连带损害方面，减少被入侵域名造成的伤害。

是的，确实需要报告人提供更多的证据，不过也需要应对问题的整个链条的更多参与。

格雷姆 • 邦顿： 谢谢，克里斯。内容很多。

我认为你说的完全正确，在这方面要做的工作还有很多。而且还快速超越了注册服务机构和注册管理机构的责任和专业知识，进入了托管服务公司等领域。我想回到一个问题上。

不过首先有请艾伦发言。

艾伦 • 伍兹： 实际上，在克里斯后面发言，我的发言会很短，我只想说一件事，一件让我和克里斯都感觉惊讶的事情。那就是 SAC 115。我们谈论的是互用性，确保特定的运营商能够在正确的时间参与进来，从而确保及时响应，因为我们的目的是维护域名的存活时间。我们牵涉的范围越小，造成的危害也就越小。

如果在错误的时间联系了错误的提供商，那么这种牵涉范围就变大了。我们需要尝试避免出现这种情况。所以我们应该明确对 DNS 滥用的研究以及未来的工作方向。我对此很期待。期待着能够将我的后台与你们的后台连接起来，共同努力。

不过我想指出的一点是，某些注册人，当然是来自大平台的注册人，他们自己就有非常精密的滥用监测程序，这一点我刚刚忘记提了。

我想刚刚克里斯也稍微提到了一些。

我们不会关闭 facebook.com，这里只是举了个最明显的例子。我要说的是，我不是 .COM。我们不会因为 Facebook 上的滥用情况而关闭 facebook.com。那会很荒谬。我也认为我们需要考虑方案的平衡性。

格雷姆 • 邦顿： 谢谢，艾伦。

这里有个问题出现过几次了，我想再次请艾伦和雷格回答，因为我认为这需要一些社群合作，这个问题是：作为注册管理机构和注册服务机构，你们与托管公司的关系是怎样的？因为我的感觉是，很多人都觉得你们的关系相当紧密。我不打算代你们回答，我认为在很多情况下并不是这样。

当我们谈论这个的复杂性，以及克里斯谈到的，在注册人、托管公司、注册服务机构、注册管理机构之间的升级路径，那些关系清晰吗？那样的流程中存在标准吗？这是个我们应当做更多工作的地方吗？有请雷格。

雷格 • 利维： 谢谢你，格雷姆。

重申一下，我的回答将以 Tucows 这样的批发注册服务机构的事实情况为依据。

所以答案可能不一定代表其他注册服务机构。我们没有任何托管服务，因此才有了 Exact Hosting。在我们的那家子机构中，有大约 500 个网站。从本质上说，我们没有托管。

[笑声]

我们的分销商通常也是托管公司。所以经常在这种情况下，我们可以联系到分销商，告诉他们这个网站被入侵了，然后他们就会进行处理，甚至不需要注册人介入。当我们的分销商是托管公司时，我们的关系就很紧密。

但情况并非总是如此。托管公司有很多。我的意思是，托管是一种需要域名的服务。但它可以完全独立于提供域名注册的服务。

所以当我们的分销商不是托管公司时，事情就有些棘手了。我们需要使用一种分散化信息群 (DiG) 工具来找到托管公司，然后也只能根据从 DiG 工具获得的信息来联系托管公司，就好像其他互联网用户那样。

格雷姆 • 邦顿： 抱歉，我的鼠标光标不见了。

谢谢雷格。在我发表评论前，先有请艾伦发言。艾伦。

艾伦 • 伍兹： 谢谢！再次向我们的译员说声抱歉。爱尔兰人总是语速很快。

站在注册管理机构的角度，其实更难。我们与托管服务提供商之间没有联系。当我们面临问题时，倒是很希望能够有所联

系。我们也可能让我们的注册服务机构伙伴看看他们是否能够联系到，或者他们是否就是托管服务提供商。

我想说的是，不过 — 我的狗狗也在打鼾了。

我想说的是，我们在尽力与他们展开合作。很明显，我们有很多不同的交流对话。其中一个是在 ICANN 范围内的，也有一个是关于互联网与管辖权的，我们全都身在其中，在那些讨论中，托管服务提供商也参与了，正常情况下他们并不在 ICANN 范围内。我们可以进行这些对话，在互联网与管辖权方面，与托管服务提供商建立更多桥梁。

我认为对我们重要的是，将这些心得和经验带回 ICANN 社群，让大家知道我们在做什么。我认为这是我们可以做得更多的地方。这就是发生的事情，要知道，互联网和管辖权的定义进入了合同各方，是我们的共同努力。

所以我们在尽可能多地与托管服务提供商合作，将了解到的经验成果带回 ICANN 社群，这对我们注册管理机构而言也非常重要。

格雷姆 • 邦顿： 谢谢，艾伦。我的感觉是，有很多注册服务机构都提供托管服务，但也不是全部。但在确定与托管服务提供商建立联系时，

需要考虑的是在全世界范围内他们的数量，所以这种关系并不一定很常见。所以我们需要考虑的一个真正的障碍就是，我们要如何改进向托管服务提供商报告的流程。我们将要有更多的工具供他们使用，也要有更适合的行动场所。那么当注册人或托管服务提供商没有响应时，我们应该如何为注册服务机构和注册管理机构定义升级路径？现在我们需要重新评估报告上来的滥用投诉。

我看到洛里举手了，我们还剩余 18 分钟时间。所以我想，我们随后将直接进入问答环节解决问题。
有请洛里。

洛里 • 舒尔曼： 谢谢！我想重申一些观点，回应聊天框中的内容。

不过我确实认为，在报告、互用性、创建安全空间等方面，值得讨论一下多少投资是合理的，以及在两种缓解技术方面能够或应该预期些什么。那可能是人。

根据雷格的发言，AI 扮演了很广泛的角色。欧洲互联网域名注册管理机构 (EURid) 也毫不讳言他们的 AI 工作。但我们仍然需要一个由人组成的队伍来检查 AI。没有人认为结果是理所当然的。它们都在意料之中。我们都理解，至少在我的选区，大家都理解，为了创建一个更加安全的互联网，需要大量的投资，

实际上我们付出的代价要更高。我们想要讨论那个吗？我知道，这是公民社会特别关心的问题，在那里，域名的价格保持相对便宜，对于任何需要域名并想要建立合法网站的人来说都是可以接受的，这一点很重要。

但与此同时，我们知道有一些注册管理机构和注册服务机构正在加大投资。那些投资全部到位了吗？我认为这是社群可以问问自己的一个重要问题。

格雷姆 • 邦顿： 谢谢，洛里。事实上，我认为这或者可以很顺畅地切入到下一组问题，它们与问答功能和聊天框里的内容有关：社群应发挥什么作用？ICANN 是否发挥作用尝试解决今天我们发现的这些挑战？那可能会成为应对恶意注册的最佳实践。ICANN 对被入侵网站的权限范围是什么？我们可以做些什么？社群中有什么地方？有很多关于 DNSAI 的，不过我想等下再讨论。

我想知道我们的专家组中是否有人对这个社群的未来有什么想法。我也听不到罗德了。我想知道你们有没有什么想法。雷格，我看到你举手了。

请发言。

雷格 • 利维： 谢谢。我绝对认为 ICANN 合规团队有职权对没有针对 DNS 滥用采取行动的合同强制执行。这就是说，针对 ICANN 职权内的内容，例如不包括非法内容，或前面讨论的 CSAM，而是针对 DNS 滥用。ICANN 应该更好地利用这些条款并执行它们。

格雷姆 • 邦顿： 谢谢雷格。接下来有请罗德，然后是克里斯。

罗德 • 拉斯穆森： 我来回答这个问题。我在问答功能中回答了一个类似的问题。我想这个问题来自于法夫里西奥。

实际上 SSAC 在 SAC115 谈到过，ICANN 组织乃至更广大的 ICANN 社群，包括签约方机构以及每个参与这项交流对话的人，都要发挥作用。但那是个更广泛的话题领域，而我们专注于 DNS 滥用。这是互联网上的滥用问题的一部分。我们今天谈到的一些挑战围绕着哪些适当的服务提供商参应与到缓解危害中来，无论是因为被入侵还是恶意注册造成的危害，这本身是个非常好的对话空间，但是也要想想证据标准、多长时间，或者对所报告的滥用情况的确认和缓解，可以采取哪些行动。所有这些话题都属于更宽泛的范畴。

我们正在缓步前行。大家知道，我们有很好的方案，例如域名滥用 — DNS 滥用研究所，以及互联网与管辖权工作组正在完

成一些工作。为了建立某种标准，最佳实践，等等，我们付出了大量的努力，但我们还没有做到这一点，我们还有很长的路要走，尝试创造一个生态系统，在这个生态系统中，人们可以对程序、相称性和其他你需要的东西有所期待，从而创建一个更好的应对和预防系统，以处理所有性质的滥用问题。

我认为重要的是，作为 ICANN 社群，我们在很大程度上要保持一致，随后也要与更广泛的互联网社群就如何处理这些问题进行接触，因为如果我们都只是尝试解决我们各自的独特挑战，最终将出现许多不同的系统。有很多有针对性的工作正在进行，ICANN 可能发挥作用成为一个促进对话的地方，因为虽然他们拥有资源，并汇聚了多方努力，无论是托管还是电子邮件等，但不一定有这样的优势。

因此，我强烈鼓励大家关注 SAC115，并参与一些正在进行的对话，积极主动地思考 — 在全球范围内思考如何处理这些问题，并创建我们需要的那种框架，以便再次设定期望并贯彻执行。

谢谢。

格雷姆 • 邦顿： 谢谢，罗德。

我看到已经有人在聊天框中发了 SAC115 的链接，我将会确保大家都收到链接。

有请克里斯发言，然后是艾伦。

克里斯 • 路易斯-埃文斯： 好，谢谢。我是克里斯 • 路易斯-埃文斯。

我同意罗德说的每一句话，我最初想表达的是，我同意里奇围绕合规性的发言。不过要知道，我们在如何应对 DNS 滥用方面有（听不清），这次对话交流就是其中一部分。我认为我们目前没有适当的流程来应对被入侵的域名，这也是我们开展这对话的部分原因。设定某种最低预期并形成文档，以便让客户衡量响应情况，我认为将会非常有帮助。还有，将这些标准传达给所有的注册服务机构和注册管理机构，以便他们理解对他们的要求，我认为也非常关键。包括给他们的教育培训资料。大家知道，我们前面提到过，注册服务机构和注册管理机构有很多不同类型，让他们了解如何应对是最重要的事。

因此，ICANN 可以做很多事情来将这个推广到整个 ICANN 版图之内。然后就是在罗德的基础之上，扩展到其他领域。我们这次讨论多次提到的托管公司、服务提供商，他们在处理 DNS 滥用中扮演着重要的角色。

谢谢！

格雷姆 • 邦顿： 谢谢，克里斯。

艾伦，请见谅简短，然后我们将继续回答几个问题，最后再做总结。

艾伦 • 伍兹： 非常好。我的发言会非常简短。碰巧的是，作为整个过程的一部分，甚至在我们建议召开这次全体会议之前，注册管理机构利益相关方团体 DNS 滥用问题小组实际上已经启动了一个流程来尝试发表一篇论文。格雷姆显然也参与其中。在这个特殊的时刻，他是非官方的领导者，相信我们也将邀请来自 SSAC 的人。因此，我们打算邀请罗德还有杰夫 • 贝瑟 (Jeff Bedser)，这样我们就可以进行关于恶意注册和被入侵域名方面的有力对话；正如克里斯刚才所说的那样，正在努力奠定基础。

这是一个开场。这是让我们了解到，确实有问题正在发生，也就是 DNS 滥用问题，而我们正在努力解决，但我们也需要来自各个不同方面的力量帮助我们有效应对问题。

所以让我们继续关注，希望能很快出现成果，为后续的问题解决奠定坚实的基础。

格雷姆 • 邦顿： 谢谢，艾伦。我们正在努力完成的论文就是这个话题的 TPH。我们的目标是赶在 6 月份在海牙举行的 ICANN74 会议之前完成。我想可能会在 6 月前的几天完成，我们会确保公开给社群。

较早之前，法夫里西奥在聊天中问了一个关于这个话题的问题。社群可以做什么？是否会对注册服务机构认证协议 (RAA) 进行更改来纳入我们今天所讨论出的一些最佳实践或问题？有可能。当然，我认为这是摆在台面上的。

昨天我收到一封来自于 DNS 滥用研究所的信，提到涉及 DNS 滥用问题的 DNSO 小组来询问这类问题。我自己也在这个问题上绞尽脑汁，我认为社群的角色是真正地从这些更大的问题中去掉一些非常细枝末节。我们讨论了很多关于这个生态系统的复杂性，尤其是滥用发生在被入侵的域名上时。我认为我们应该从相对容易的恶意注册问题入手，那里产生的后果相对较小，即使错了，受影响的受害者也不会很多。

所以我们可以开始思考一下，在应对恶意注册方面，哪些工作应由社群完成。我认为这也符合 ICANN 章程中的更干净的规

定。这就是我的建议，希望这回答了法夫里西奥在聊天中提出的问题。

我们来看一下，我们还剩余 7 分钟。我想给大家一个机会，看看大家是否有任何总结发言，或者是否有人想直接回答问答环节中的问题。

雷格举手了。请讲，雷格。

雷格 • 利维： 谢谢你，格雷姆。我想强调的是阿什利在聊天中说过的话；注册服务机构利益相关方团体目前正在开发一种工具，您可以在其中输入域名，它将提供关于托管公司是谁以及如何联系他们的信息。

所以敬请留意下这件事。本周早些时候，我们向注册服务机构利益相关方团体展示了这个工具，希望很快能将工具链接提供给所有人。

格雷姆 • 邦顿： 谢谢，雷格。

我认为它很重要，DNS 滥用研究所正在进行一些类似工作，也是研发一个集中的滥用报告工具。以后识别整个生态系统中各

个组成部分的流程就会很清晰了，他们是谁，如何联系他们，联系他们有什么标准等等，目前来说都还很混乱。我们可以共同做得更好，共同携手制定流程和解决联络问题，让这些变得更容易一些。我也正在完成一些类似的工作。现在还不是谈论的时候，不过以后我会跟大家分享最新情况的。

我们来看看能否快速回答一两个问题。再次表示歉意，我们现在已经积累了很多问题了。

在我阅读问题队列的时候，有没有专家组成员对我们今天讨论的主题发表总结性发言。

我看到洛里举手了。请发言。

洛里 • 舒尔曼： 好的。谢谢！

聊天内容滚动得太快，我已经跟不上了。但我想说的是，这次会议非常及时也很有必要。我想感谢组织方邀请 IPC 和我参会，因为这次会议真的凸显了一些棘手的问题。

我认为大家面临的情况都不简单。这不是个容易解决主题。我也认为没有人会轻率地做出决定，尤其是针对被入侵的域名，至少我坐在这里听大家讨论后，我相信没有人会轻率地做出决

定。社区正在经历商标从业者以及执法和网络安全专家多年来一直都知道的事情，即每个滥用案例都可能有自己的事实模式。每个滥用案例都可能有一个更好或更坏的补救办法。每个滥用案例都要考虑自身的事实情况。

所以说了这么多，我很清楚，作为一个社群，我们有责任建立规范。这就是我认为像互联网与管辖权这样的项目，像 SSAC115 这样的文件，以及你正在做的工作，格雷姆，真的有助于建立这些规范。

但下一步是什么，我认为应该说，社群外的规范是如何建立的，以及它们在 ICANN 内部是如何运作的？在我的选区进行的讨论中提出了一个非常有远见的建议，就是当我们有网络问题的时候 — 对不起，20 年前就出现了网络抢注，当时没有司法系统或裁决者来帮助处理这些案件。我们发现了足够多的共性，于是我们开发了统一域名争议解决流程 (UDRP)，它已经运行了 20 年。

现在是时候针对被入侵的域名思考类似于 UDRP 的流程了。我把这个问题留在这里，我想这是一个未来的问题，当我们讨论解决方案和规范时，值得拿出来讨论。

格雷姆 • 邦顿： 谢谢洛里。感谢你的发言。未来这个词也很棒。

在请艾伦发言之前，我想简单地回答一下格里芬在聊天中提出的一个问题，我想我们已经谈到了其中的一部分，那就是社群内部的工作，作为一个经营着致力于解决这个主题的研究所的人，而且知道还有其他几个人在共同努力，对我来说 — 很明显，滥用问题很快就会从 ICANN 的职权范围蔓延出来，我们需要与托管方接触。我们有几个组织正致力于解决类似的问题，如全球网络联盟、互联网与管辖权(I&J)、DNS 滥用研究所，来自 eco 的 TopDNS。我们需要做的是，研究出如何有效开展合作。总体而言，我认为我们支持多利益相关方模型，而 ICANN 确实也看到了这样工作的重要性。

但我们也需要理解，相邻的组织可以超越这些边界，以一种可能不适合 ICANN 或 ICANN 系统规则的方式，与更广泛的社群接触。

所以能够向外部利益集团，例如世界各地的监管机构，以及社群内的 ICANN 解释，社群内部存在产生合规要求和 PDP 之类的工作的一席之地，也可以让行业制定最佳实践，接触邻近的事物，如托管服务、电子邮件提供商之类的社群，所有这些都可以展开合作。我们需要在这方面做得更好，因为这将使每个人受益，并解决一系列这样的问题。

我们还剩一分钟。看起来要由艾伦做最后的发言了。

艾伦 • 伍兹： 我只是想附和你说的话，格雷姆。我认为这很重要，我不同意洛里的观点。事实上，对于她说的大部分内容，我都同意。我认为，我们需要确保 UDRP 能够有效地解决域名问题。我们要解决的问题，正如格雷姆所说，是比注册服务机构、注册管理机构更宽泛的问题。我们讨论的是托管服务提供商，ICANN 系统的另一方。比 ICANN 更宽泛，但肯定属于 ICANN 的组成部分，做好我们自己部分，然后与他人合作才是解决问题之道。我想这也是我们此刻正在推动的，我们理解这属于互用性范畴。我们需要获得支持和全部理解。我们会越来越好的。我认为我们肯定会越来越好。我们必须持续改进。

格雷姆 • 邦顿： 谢谢艾伦。

现在时间已经到了。非常感谢我们的讨论组成员们。很感谢你们抽出时间参加讨论。马切伊，感谢你的精彩演讲。各位，你们很好地遵循了今天的主题，并发表了远超我们能够处理的讨论。很抱歉。我们会试着记录一部分，看看以后有没有机会纳入其他会议或工作中。

现在，我想我们可以结束今天的会议了。再次感谢各位参与讨论。非常有价值。

[会议记录结束]