SAN JUAN 一 工作原理：了解 DNS 滥用
大西洋标准时间 2018 年 3 月 12 日星期一 一 13:30 至 15:00
ICANN61 | 波多黎各圣胡安

男性发言人（姓名不详）： 大家下午好。ICANN 第 61 届会议。3 月 12 日。工作原理：了解 DNS 滥用。

凯西 • 彼得森 (CATHY PETERSEN)： 大家下午好。我们将在几分钟后开始举行“工作原理：了解 DNS 滥用”会议。谢谢。

诸位，下午好。欢迎参加“工作原理：了解 DNS 滥用”会议。我们有幸请到了首席技术官办公室的卡洛斯 • 奥法瑞兹 (Carlos Alvarez) 提供本场会议的主讲嘉宾。卡洛斯？

卡洛斯 • 奥法瑞兹： 非常感谢，凯西。谢谢所有前来现场参加会议的各界人士，以及通过在线方式参会的所有人士。现在好像有 23 人在线，我想等下随着会议的举行，应该会有更多人上线来。

今天我们将讨论一个很重要的话题。这个话题与每个人都息息相关。同时，从某种角度来说，这个话题很有争议性，值得所有人关注。这个话题就是“DNS 滥用”。

首先，我们来看看大家讨论这个问题时提出的各种观点。大家提出了很多不同观点。大家会从不同的角度理解 DNS 滥用。我们先了解一下这些观点，然后讨论几个 DNA 滥用或误用案例。我们还将讨论不断进化的互联网格局与 DNS 的关系。最后，我们将在 ICANN 背景下讨论 DNS 滥用。

首先值得指出的是，人们对于什么是 DNS 滥用并没有形成全球统一的定义。在这张幻灯片上，大家可以看到人们对于网络犯罪、骇客袭击和恶意行为等热门话题有着各种不同的定义。

我们可以将 DNS 滥用归为三大类：数据损坏、拒绝服务以及隐私问题。当然，DNS 误用和 DNS 滥用也是两个不同的问题。我向大家读一下这张幻灯片上的内容。滥用是指蓄意利用 DNS 实施欺骗、密谋或未经请求的活动，或者用于擦除或解析域名的流程。我们稍后会阐述这句话的意思。我们稍后再说。

对于定义什么是 DNS 滥用或者通过各种要素来理解 DNS 滥用，GAC 有什么看法？对于这个广泛的问题，GAC 有什么意见？GAC 在一份有关如何缓解滥用活动的文档中发表了一份公报，其中提供了我们目前已应用至所有新 gTLD 的若干防护措施。其中提到了特定的滥用活动，例如分发恶意软件、控制僵尸网络、网络钓鱼、盗版、商标和版权侵权、欺骗和误导行为、假冒行为，以及其他各种可能违反适用法律要求的活动。

这些内容看上去很宽泛，对于其中某些主题，有人认为其实算不上是对 DNS 技术系统的技术性滥用。但是，如我之前所说

的，我们现在只是介绍社群成员对此问题的各种观点。这是观点之一。还有人根据各种理由认为商标和版权侵权，以及特定情况下的欺骗和误导行为也算不上对 DNS 的技术性滥用。

关于发送垃圾邮件是否属于域名系统滥用，这是一个重大问题，但我不准备在本次会议中对它盖棺定论。

在运营和安全社群以及执法部门看来，发送垃圾邮件是其他恶意活动的迹象和先兆。就其本身而言，至少时至今日，它还不被人们视为对 DNS（也就是全球域名系统）的技术性滥用。

在进行威胁研究和数据分析时，你可能发现有人发动了一次垃圾邮件行动，并识别到对方所使用的作案基础设施。如果继续跟踪对方的活动，你早晚（通常很快）会发现他们会对所发送的垃圾邮件实施跟进。这些跟进活动可能是分发恶意软件，分发虐待儿童的材料，也可能是网络钓鱼，类型可能五花八门。简而言之，DNS 滥用是指攻击或滥用 DNS 基础设施的任何行为。我将通过一份演示幻灯片来介绍这个问题。

我们可能发现许多种 DNS 滥用方法。我在这里准备介绍其中两种。第一种是滥用域名解析，这是用于将域名转换为 IP 地址的技术方法。第二种是域名注册，试用注册服务协议。

犯罪分子可能以各种方式滥用注册管理机构和注册服务机构提供的服务。我们也将讨论这个问题。

DNS 误用是指在更高明的技术层面上利用 DNS 协议，或者出于恶意目的利用注册流程。我们稍后将详细解说这些问题。[我的目标] — 是的。这里。

抱歉。你不需要阅读所有这些幻灯片。我的目的不是这个。我的目的是从一个简化尺度向大家展示 DNS 的运营要素。

顶部蓝色文字显示的是权威域名服务器，其中托管着每个域名或 TLD 的权威数据。正下方是递归域名服务器，你可将其视为 ISP 允许你使用的 DNS 服务器。ISP 是指为你提供互联网接入服务的公司。他们为你提供 DNS 解析服务。

下面还有客户端或者根解析器。什么是根解析器？它就在这里。它是我们浏览器中的一种函数，举例而言，它可以寻找相关信息，以便它自己能够使用我想要使用的资源。

例如，如果我在浏览器地址栏输入 www.ICANN.org，系统便会调用根解析器函数，将域名解析为 IP 地址，而 www.ICANN.org 的内容就托管在那个地址中。它会将内容下载到我的设备中，以便我查看、互动或者执行其他操作。

DNS 的这三个运营要素都是潜在的攻击目标。基本上，所有在线内容都是潜在攻击目标。

例如，这就是它有意思的地方。让我们重点关注反射/放大，这是DDoS（也就是分布式拒绝服务）攻击的核心。

什么是反射？反射的意思是，你可以发送一个数据包，并伪造源 IP 地址信息，让服务器认为它是来自其他地方，从而让服务器向另一个 IP 地址发送响应。因此，如果我的目标是攻击凯西，我会向 DNS 服务器发送一个数据包，并将数据包的 IP 地址伪造成来自凯西，而不是我。

如果我使用开放式解析器来实施攻击，开放式解析器是一种互联网上到处都有的 DNS 服务器，少说也有成千上万个，它不会过滤查询的源 IP 地址，它会响应全球任何地区任何用户的查询，所以凯西会收到海量数据，因为我将向互联网上那成千上万个开放式解析器发送 DNS 查询。所有这些解析器都会认为那些查询是来自凯西，因此会全部予以响应。这就是反射。

另一个攻击矢量是放大。放大是什么呢？放大的意思是，我发送的每一个查询本来都很小，通常只有一行命令，可能简单到仅包含 dig 域名服务器，域名，没了，就是这些内容，只有七个字节。真的非常小。它只是一行文本，但其响应将变得很大，可能产生 2.3、2.5 或者 2.7 兆数据。将这个数值乘以我通过僵尸网络发送的成千上万个查询，你们说将会造成什么结果。大家还记得僵尸网络是什么吗？就是犯罪分子控制着的由被攻陷设备组成的庞大网络。这个网络中可能包含成千上万台被攻陷的设备。控制着僵尸网络的犯罪分子可让所有这些被攻陷的设备向互联网上的所有开放式解析器发送查询，从而让那些解析器向凯西发送海量响应。

我控制着由大量被攻陷设备组成的僵尸网络，加上我利用成千上万个开放式解析器，以及我发送的特殊命令（也就是 dig 查询），这会产生倍增效应。Dig 是一个用于从 DNS 获取信息的命令，它会触发响应。就像我刚才提到的，这个命令的编写方式令其会产生体积很大的响应。

所以凯西如果没有部署 DDoS 保护之类的防御措施，便可能会被挤下线。如果她的设备承受不了疯狂涌来的流量，她就会离线。这种攻击无法被阻止。

业内第一场将 DNS 作为攻击矢量的大规模 DDoS 攻击 [听不清楚] 发生在 2003 年，受害者是 Spamhaus。Spamhaus 是一家致力于反垃圾邮件和恶意软件事业的组织。他们致力于调查互联网，向大家提供有关如何缓解威胁和实施保护的各种数据。

当然，攻击手段在不断进化。现在，DNS 绝非唯一的攻击矢量，而只是其中之一，但作为一种协议，它经常被用于实施攻击。

我们还将讨论缓存投毒攻击或资源耗竭攻击。这是我们要讨论的倒数第二种攻击矢量。最后一种是 DNS 中间人攻击。在介绍该攻击矢量之前，我们将看几张幻灯片。

这就是我们刚才说的。这次大规模 DDoS 攻击通过反射攻击矢量，向开放式解析器发送伪造了源 IP 地址的数据包，令其误以为发出查询的是凯西的设备。这些解析器收到的查询将触发

体积很大的响应。这就是放大攻击矢量。凯西将收到海量响应。正如我刚才所说的一样。

但这不是我干的。事先声明一下。我咖啡喝太多了。我们说到哪里了？

这里。另一种攻击 DNS 的方法是利用他人的域名服务器。域名服务器是域名解析基础设施的一部分。因此，如果我要擦除你的 carlos.whatever 域名，我就要最好设置至少两个服务器，DNS 是一个全局系统，用于获取有关我为该域名关联的资源的信息。换句话说，我将定义那些信息并将其提供给域名服务器，这些信息就是 IP 地址；简而言之，就是我的邮件服务器、web 服务器以及 FTP 服务器等的位置。

如果有人将我的域名服务器挤下线，那么任何人都无法继续访问其中的信息，这就意味着我将无法接收或发送任何电子邮件。他人将无法访问我的网站等，因此，如果域名价值很高，这会导致重大后果。我不是说那个 carlos.whatever 是一个高价值攻击目标，它可能并不存在，但我们不排除日后有这种可能。

就这种攻击类型而言，犯罪分子便是在滥用 TCP 协议。我们向服务器发送 TCP 数据包时，服务器会作出响应。简而言之，当服务器响应 TCP 连接时，发起连接的设备和响应的服务器将建立握手，从而在两者之间创建一个持续的通信通道。这意味着两者都必须分配特定资源以用于维持该通信通道。

如果你控制着一个包含大量被攻陷设备的僵尸网络，并通过那些设备同时向域名发送响应/查询，那么你就会迫使服务器建立大量 TCP 握手，令其不得不分配大量资源来维持 TCP 通信通道，这样一来，服务器迟早会再无资源可供分配给更多 TCP 连接，从而导致任何用户都无法向该服务器查询 DNS 信息。服务器还是会在线，但无法响应任何查询。即如幻灯片上所说的，域名解析服务的性能将会下降或者发生服务中断。

运气好的时候，你能够在几分钟后得到响应。但对于大流量域名，或者如果解析服务发生中断，那就需要漫长时间才能得到响应了。当然这是一种极端的情况，所有人都会想办法予以避免。

缓存投毒攻击。这个比较复杂。犯罪分子会花招百出，通常都是这样。还记得之前一张幻灯片的内容吗？顶部是权威域名服务器，例如我创建并注册 carlos.whatever，然后关联 ns1.carlos.whatever 和 ns2.carlos.whatever 来提供 DNS 以及我的邮件服务器和 web 服务器等所关联的信息。那就是我的权威域名服务器。

市场上有很多 DNS 提供商，例如 9.9.9.9、8.8.8.8、OpenDNS 或者 UltraDNS，而很多 ISP 都是递归性的，他们会代表用户发起查询。大家都知道，在这些递归解析器中，有些没有得到妥善保护，他们易于受到攻击。设想一下，世界各地有成千上万家互联网服务提供商，其中一些是由不具备大量资源的小型公

司运营。他们拥有运营基础设施，但没有足够的资源来保护它们。

当那些服务器没有得到妥善保护时，犯罪分子便可能通过许多方式攻陷它们。例如，如果我是某个 ISP 的用户，而这个 ISP 的递归解析器已经被攻陷，那么当我发送查询以查找各种网站（例如 PayPal.com）关联的数据时，我可能得到正确响应，但由于服务器已被攻陷，犯罪分子可能会在数据中添加额外的信息。那些额外信息可能显示：“顺便说一下，BankOfAmerica.com 的 IP 地址是这个。”

然后它还会自动更新我的设备的临时内存，也就缓存。在我的设备中，它可能成为宿主文件。发生这种情况时，你们猜我下次访问 BankOfAmerica.com 时，我的设备将转到哪里去？如果在指定时段中发生这种情况，我的设备将转到犯罪分子希望我访问的 IP 地址。这就是一种很糟糕的情况。情况很不妙。

然后会怎么样？我就会访问犯罪分子运营的服务器。我会看到他们希望我看到的内容，在这种情况下，我可能看到模仿美国银行官方网站的钓鱼网站。这时，我可能会很开心地输入我的用户名和密码，那我的个人财产可能就要遭殃了。

犯罪分子还可能通过其他方式发起这种攻击。他们可以直接攻陷你的设备，并修改你的 DNS 配置。我们稍后将通过示例介绍一个大约在四年前被瓦解的恶意僵尸网络。如果我的设备配置为向 1.1.1.1 之类的地址发送 DNS 查询，他们可能在这里或

者通过笔记本电脑更改这个 IP 地址，将用户想要访问的合法 IP 地址改为他们的恶意地址。他们可能提供一个他们运营的 DNS 服务器的 IP 地址，而这个服务器可能配置为提供他们自己的基础设施的 IP 地址。换句话说，他们将让设备被攻陷的用户访问他们的恶意网站。我们会稍微谈一谈这个问题。

在这种情况下，就缓存投毒攻击的方式而言，他们可能让用户的被攻陷设备向他们的 DNS 服务器发送查询。假设我要访问一个与犯罪分子无关的网站，一个新网站，但实际上任何网站都可能与犯罪分子扯上关系。我们假设这个 news.whatever 与犯罪分子没有关系。与上个示例一样，他们会在他们的服务器发送给我的设备的响应中额外添加一些信息。那些额外信息可能只是一个 IP 地址，例如“顺便说一下，我们的银行网站的 IP 地址是这个”。如果我在指定时期中向该银行域名发起查询，比如我想访问某个网上银行，这时候，砰！一 我会进入犯罪分子的网站。这时我的个人财产可能会遭殃。

我刚才说的这种恶意软件就是 DNSChanger。那恰好就是我说的这种情况。它会更改用户预期的 DNS 配置。这种攻击很普遍。操控这种僵尸网络的犯罪分子可能会获得很多钱。僵尸网络正是这种攻击矢量的核心。根据某项执法行动的结果，执法部门通过有力证据证明那些犯罪分子非法获得了 2500 万欧元。这个数字可能只是冰山一角，但执法部门当时通过证据只能证实这些。

借助 DNSChanger，犯罪分子能够更改用户设备上的 DNS 配置。他们可以通过替换用户进入网站时会看到的广告，弄出一些看似无害的内容。如果某天早晨我在办公室登录我的首选世界杯新闻网站时，没有看到合法内容，而是看到了广告，那就是他们替换上来的。这会给他们带来持续性收入。这种情况很早就出来了。这种手段已成为他们的印钞机。

它没有什么害处，或者说看起来如此。用户在设备上不会看到任何异常行为。他们还是能够访问自己想要访问的内容。他们还是能够与互联网以及他们想要的资源进行互动。不会看到明显的异常情况。

但实际上是有异常的。由于感染的设备数量众多，人们产生了担忧，因此决定发起这次行动。我不记得具体的设备数量了，但这个僵尸网络中确实包含来自多个国家和地区的数十万台被攻陷设备。我也没什么好隐瞒的，此案大约涉及 20 个国家和地区。但我不能完全肯定。

所以问题来了，执法部门的人需要处理犯罪分子运营的那些 DNS 服务器。他们要么将服务器关闭，如果是这样，你们觉得他们关掉那些 DNS 服务器将导致发生什么事？如果所有用户设备都向那些服务器发送 DNS 查询，将发生什么情况？

用户可能认为他们丢失了互联网连接。他们的设备仍然连接着互联网，但无法解析任何域名，因为那些 DNS 服务器被关掉了。所以他们不能直接关掉那些服务器。

他们还可以通过工程手段替换那些服务器。法庭通过国家计算机紧急事件响应小组和各种技术在某个时段中为那些服务器安排了一名管理员。同时在涉案司法管辖区开展教育宣传活动，让用户意识到他们必须清理自己的设备。

当然，从那时起，犯罪分子也不甘心失败，他们找到了许多其他滥用 DNS 协议的方法，以及不同的 DNS 运营要素，其中一些还很有意思，至少从学术研究角度看是如此，因为它们显示出了创造性，虽然是出于恶意目的，但确实很有创意，例如隐秘渗透通道。这些内容应该是在下一页幻灯片上，哦，不在。让我们来讨论这个。

你通过被攻陷的网站发送数据，而网络管理员没有意识到数据失窃，这就是所谓的隐秘。DNS 之所以能做为一种很有意思的隐秘渗透通道，是因为用于 DNS 通信的端口通常没有被屏蔽。它不能被屏蔽。

网络流量需要通过该端口在不同端口之间流动。DNS 协议使用的端口是端口 53。虽然工程师能够通过多种方式在内部网络中重新分配该端口，但操作起来比较复杂。所以人们一般没有重新分配这个端口，或者将它的功能移动至其他端口。这就意味着流经端口 53 的流量无法被屏蔽。重新分配这个端口的操作很复杂，因以它无法被屏蔽。如果被屏蔽，那么人们将无法进行 DNS 解析，所以大家也就习惯这样了。

隐秘渗透通道是如何运作的？它有多种运作方式，至少据我所知就有两种。第一种方式：犯罪分子攻陷一台设备，然后通过该设备缓慢地向犯罪分子的域名服务器发送 DNS 查询。具体方法是，在每个 DNS 查询中，犯罪分子都会将最不相关位元替换为对应于他们要渗透的数据的位元。如果工程团队或者网络管理员检查这些查询，也就是检查流量，它们看起来仍是 DNS 查询。他们需要收集到用于渗透特定数据块的所有 DNS 查询方能查出真相。基本上，这需要用到分析功能。意识到最不相关位元被修改后，他们要汇总那些最不相关位元并进行分析，然后才能发现渗透的对象。那是一种方式。

犯罪分子利用 DNS 渗透信息的另一种方式是通过 TXT 记录，这种方式较为简单。创建域名时，你会默认成为区域文件的管理员。

我们在域名的区域文件中定义域名关联的资源，其中包括网站、邮件服务器以及 FTP 服务器的信息。如果你签署了域名 DNSSEC，这些信息便会进入这里。如果你采用所有相关技术来保护客户或者公众，也许你们有些人听说过这些技术，不好意思，大多是些缩略词，这些技术包括 SPF、DKIM 和 DMARC，简单来说，这都是些用于保护用户的技术。

所有那些信息都会进入 TXT 记录。你实际上可以将所有信息都保存到 TXT 记录中。可以保存到 TXT 记录中的信息类型没有任何限制。都是些纯文本。犯罪分子还能够利用这些 TXT 记录来

渗透信息。他们可能向域名服务器发送包含有关 TXT 记录信息的 dig 查询，以便收集相关信息并加以组合，然后对渗透的数据加以利用等。

快速通量，大家平时可能是用这个术语。如果不是的话，我们回头再确认，我记得应该是这个术语。

域名注册是很受攻击者喜欢的目标。这很明显。不幸的是，犯罪分子和恶意操作者会滥用 gTLD 和 ccTLD 空间中的合法域名注册服务提供商。他们很喜欢滥用注册服务机构和分销商。他们会获取大量域名。这个问题解决起来很麻烦。较低的域名价格会吸引恶意操作者，我觉得这是人性使然。越便宜越好嘛，他们会注册更多域名，就像降价能够吸引更多合法注册人和用户注册域名一样。这是人性使然。那并没有错。只是要看怎么利用。

自动注册域名将 一 重申一下，这件事本身也无所谓对错，就看行业是怎么用它，我们当然可以用它来操作大量的合法域名组合。

然而不幸的是，犯罪分子也可能滥用它。就这个问题而言，我想到了 DGA 域名，这是犯罪分子掌握的一种用于创造和注册大量域名的自动化技术。

什么是 DGA？就是域名生成算法。设想一下僵尸网络。所有僵尸网络都必须拥有一个命令与控制基础设施，以便犯罪分子精确指挥和控制其恶意基础设施。

如果该基础设施发生故障，将会发生什么情况？他们会制订计划 B、C、D、E、F、G 等等。这就是 DGA 的作用。当僵尸网络意识到其中一个与命令和控制有关的服务器当机、暂停、没有正确定义或者发生其他情况时，一 它会注册一个新的服务器。这仅仅是一个例子。DGA 行为简直五花八门。这只是一个简单示例。砰！它会在任何 TLD 下注册任何字符串，然后离线运行。

如果僵尸网络的命令和控制功能因威胁缓解措施而发生性能减退，那么那个新的 DGA 字符串注册会如何？砰！又来了，他们将丢失命令和控制功能，但会继续运行。

我们来讨论一个很有意思的案例。希望就快翻到这一页幻灯片了。攻击者和犯罪分子为什么要给各种事物注册域名？他们会给任何你们能想到的东西注册域名，以用于网络钓鱼、分发勒索软件和恶意软件、散播流言蜚语、出售伪造商品和非法药物等等。

最后一行是命令和控制功能，这是为了保护稳定性和弹性。我也不知道它为什么显示成那样。鉴于攻击规模，这是最重要的考虑因素。

有时候，人们对于出售非法药物是否属于 DNS 滥用会有些疑问，因为从技术上来说，它与 DNS 滥用不相关。它更像是出售假货的网站。这倒也没错，但有时候问题的表面下会另有一番景象。我无法和大家详细讨论，但请注意，有时候问题的表

面下会另有一番景象。我们可能只是看到有一批网站在出售特定司法管辖区认定的非法药物。但从深层次来说，它会给许多人造成危害。

你有问题要说吗？麻烦靠近其中一个麦克风。

凯西 • 彼得森： 请随意使用桌面上的麦克风。请报出自己的姓名和附属机构，如果你有组织的话。谢谢。

法尔扎内 • 巴迪 (FARZANEH BADII)： 我叫法尔扎内 • 巴迪。我是非商业利益相关方团体的主席。我以个人身份发言。你刚才提到出售非法药物的域名可能导致其他危害，你是指可能发生技术滥用吗？还是在说网站的内容？

卡洛斯 • 奥法瑞兹： 我是指他们可能利用域名进行非法运营。他们可能利用域名发布网站内容，随后还可能实施更多犯罪活动

法尔扎内 • 巴迪： 我补充一下。所以这个方面与 DNS 无关，只是涉及技术运营？

卡洛斯 • 奥法瑞兹： 他们会出于这个目的利用域名。

法尔扎内 • 巴迪： 谢谢。

卡洛斯 • 奥法瑞兹： 当然。

我能破解的话，为什么还要花钱买，对吧？当犯罪分子能够破解并掌握域名时，他们为什么要花钱买呢？

有时候，犯罪分子会选择攻陷并劫持域名，而不是注册域名。他们如何实现这个目的？他们可以破解用户凭据。他们可以破解注册人用于访问控制面板的凭据。控制面板是注册人用于管理域名的 web 接口。

设想一下，犯罪组织想要接管一个特定的高价值域名，或者危害特定银行的客户。他们可能只需针对银行员工发动一个单纯的网络钓鱼行动，通过某些社交工程手段诱使银行员工点击他们本不该点击的链接，然后窃取对方的访问凭据。

随后，犯罪分子便可以为所欲为了。他们可以简单地在你看到的二级域下创建三级域。如果银行遭遇这种情况，假设我的银行是 carlosbank.whatever，犯罪分子可以创建一个“I’llphishyou.carlosbank.whatever”，然后在网络钓鱼行动中发送电子邮件更成功地诱使受害者点击，因为他们看到的二级域确实是银行的真实域名。

或者他们还可以完全更改域名服务器。他们可能更改域名相关的任何信息。他们可能更改任何记录。他们可能撤下域名区域文件中的所有信息。

不幸的是，当注册服务机构没有妥善保护自己的基础设施，因而遭到攻陷时，便确实会发生这种情况。这种情况不会经常发生，但确实会发生。一旦发生，那就不妙了。所幸的是，在那些已经发生的少数案例中，犯罪分子都只针对特定的高价值目标，而且注册服务机构也快速做出了响应。实际上，这都是老黄历了。那个案例也得到了妥善处理。犯罪分子会瞄准他们事先确定能够在控制住那些服务器后掌控的目标。

当注册人被诱使点击恶意链接以及随后发生网络钓鱼攻击时，我们可以从用户角度观察犯罪分子是否得逞，或者犯罪分子是否能顺利攻陷注册基础设施。

这是网络钓鱼的另一面。有多少注册人会使用相同的控制面板访问凭据来管理域名？有多少注册人在被攻陷之前，会为控制面板设置与帐户相同的访问凭据？根据每周或每月发生的数十起攻击和大规模泄露事件，我们对于这些问题的答案不得而知。

凭据填塞攻击即犯罪分子尝试通过在之前的数据外泄活动中攻陷的用户名和密码登录尽可能多的服务。他们获得凭据后便会登录服务，并将你挤下线。这些问题的答案我们无从得知，没

办法检测。有多少注册人会使用重复密码来管理域名注册？我们无从得知这个问题的答案。这始终是一个有关意识的问题。

快速通量，在这里。犯罪分子使用快速通量技术从一个 IP 地址快速跳到另一个 IP 地址，让执法部门和威胁缓解专家的工作越来越难以开展。

他们通过在其区域文件中定义短 TTL 来实现此目的。TTL 就是存活时间。也就是与网站关联的 IP 地址的有效持续时间。在该时间后，递归解析器必须再次查询才能获得该信息。再次查询后，它们将收到一个不同的 IP 地址。看到短 TTL 时，例如 120 秒、180 秒、2 分钟、3 分钟或 4 分钟，研究员就会想：“嗯，有问题。”

需要注意的是，大型 CDN 为了保证稳定性、进行负载平衡以及出于其他技术原因时也可能使用短 TTL。CDN 就是内容分发网络。但那是另一回事。如果你是威胁研究员，您肯定知道如何区分哪些情况是大型网络在使用 TTL，哪些不是。但如果你遇到具有短 TTL 的新域名，而且它关联的新基础设施曾涉嫌发送垃圾邮件或执行其他恶意行为，那么就值得怀疑了。这时候，威胁研究员就需要拦截那些基础设施的流量，以便保护网络。

假设你是执法部门的人，你正在调查恶意操作者使用了快速通量技术的涉案基础设施/运营活动，你看到相关内容存储在这个国家的这个服务器中，两分钟后，那些内容突然又出现在另

一个国家的另一个服务器中，再过两分钟后，那些内容又变了一个位置，再过两分钟，那些内容又跳到另一个国家去了。执法部门应该如何解决这种问题？

很难解决。非常难。双重快速通量，在这里。这种技术在，怎么说呢，犯罪云服务中很常见。我们称之为 Avalanche。恶意操作者在 Avalanche 中会使用双重快速通量技术。意思是他们会频繁地更改域名服务器。

如果我想查询 carlos.whatever，那么现在我可能会查询到 ns1.carlos.whatever 去，过两分钟后，我可能会查询到 ns1.cathy.next 去，再过两分钟后，我可能查询到 ns3.cameron.yoohoo 去。域名服务器可能每两到三分钟变更一次。这些域名服务器会每两三分钟变或者根据犯罪分子的设置的短 TTL 更一次 IP 地址。这种手段比普通的快速通量更麻烦和复杂，但优秀的研究员还是能够找到并解决它们。天网恢恢，疏而不漏。

我刚才提到，DNS 可以作为一种隐秘渗透通道，它不仅适用于数据渗透，更主要是用于实际控制感染或攻陷设备用的恶意软件。犯罪分子通过 DNS 向设备发出指令。他们会修改攻陷了设备的恶意软件。他们可能通过 DNS 注入更多恶意软件。

这个问题很麻烦，因为我们无法屏蔽用于 DNS 通信的端口 53。所以我们只能寄希望于网络管理员拥有高明的技术手段，能够检测到这些攻击。

网络管理员可以通过各种技术来解决这些问题，但我无法一一进行解说，因为全部解说的话可能还要三个小时才够。我们只能希望他们，希望网络管理员能够实施那些技术。

我们刚才看过这个了。用于执行这种攻击的恶意软件有很多，我们举两个例子：Feederbot 和 Morto。大家看，僵尸网络命令与控制将指令编码到 DNS TXT 响应中。被攻陷的设备向域名服务器发送查询，而恶意操作者已将那个 DNS 服务器配置为提供 一 查询对象是 TXT 记录，而该 TXT 记录将向被攻陷的设备发出指令。指令可以是任何内容。例如“以这种方式攻击这些目标和流量。”可以是任何内容。

不断发展的 DNS 格局。DDoS 一种服务关于 Mirai。你们还记得 Mirai 吗？好的。那是一场不愉快的回忆。

Mirai 是，怎么说呢，一个由 booter 服务或 stresser 服务提供商组成的联盟通过这个僵尸网络实施了这次攻击。

什么是 booter 服务或 stresser 服务？它是一种人们架设在某些地方的网站，那些人声称自己销售系统容量以供大家测试服务器的弹性和稳定性。你付给他们一笔钱，他们声称自己提供如下服务：“我们将在这个时段向你发送一批流量，以便你测试自己的基础设施的弹性以及抵御攻击的能力。”

问题是，那些 booter 或 stresser 服务会向任何人销售服务，无论买家是不是待测试基础设施的运营方。换句话说，他们提供雇佣 DDoS 服务。我们不难找到他们。你们会在线上，你通过

搜索引擎可以轻松找到他们。他们中有些人会傻傻地接受信用卡付款，当然这对执法部门是件好事。你只需要向他们付钱，并提供想要测试的基础设施目标和相关信息，毕竟你是想要确保自己的网络有足够弹性。[听不清楚] 好的。麻烦大了。

他们会通过许多方式来执行此操作，僵尸网络当然也是其中一种。我们已经讨论了快速通量和双重快速通量。我提到了 Avalanche。我们讨论了前面几张幻灯片的内容。Avalanche 是一个很特别的案例，想必大家也明白。

物联网。我真不想提起物联网历史上的那个 V 字事件，但很不幸，它是如此真实。大家都知道，这不是什么新鲜事。

举一个好事变坏事的例子：大家还记得 2016 年 10 月 Brian Krebs 遭遇的攻击事件吗？也许是 9 月？攻击是针对 OVH，那是一家 ICANN 认证注册服务机构。他们也是法国一家大型托管提供商。他们检测到那场攻击是来自大约 146,000 台数码摄像机。

那个僵尸网络能够发送 1.5 TB 的数据。就当时而言，没有人能预见到这种情况。太疯狂了。我几乎无法在脑海中想像出那是多大的数据量。他们测量到 1.1 TB 直接涌向他们的实际流量。那可是摄像机。重申一下，这不是什么新鲜事，但值得一提。DNS 是那场攻击使用的矢量之一，不是唯一的矢量，只是实际使用的手段之一。

还有 WannaCry，刚才我们也提到了，现在我就不说了。

Avalanche 是一种云犯罪服务。设想你来到一个网站，创建了帐户并登录，然后就可以选择恶意软件类型以及想要发动的恶意行动类型。那些人将为你完成一切。你只需要向他们付钱，他们就会为你完成所有操作。他们为你提供恶意软件以便感染你的客户。他们会帮助你实际感染客户的设备。他们还会 [听不清楚] 域名，代表您完成命令和控制操作。他们可能为你 [听不清楚] 那些域名。

他们可能托管恶意软件分发站点。他们可能为你完成所有这一切。这可谓是将犯罪服务的复杂性推上了一个新台阶。

Avalanche 就是通过算法自动生成大量 DGA 域名注册。执法部门采取行动时，沿用了 ICANN 的一个流程，即注册管理机构安全请求快速处理流程。通过该流程，执法部门从犯罪分子手中收回了 832,000 个域名。

在这些案例中，通过执法部门合作伙伴与私营部门成员的通力合作，犯罪分子彻底丧失了其基础设施的控制权。他们的基础设施就像肥皂泡一样消失了。我的意思是，东西当然还在，但他们已经无法染指。他们无法继续控制。这种感觉真的挺好的。

这些是 Avalanche 可能通过僵尸网络出于命令与控制的目的创建的部分字符串。所有那些 830,000 个域名都是在许多 TLD 下创建的，包括 ccTLD 和 gTLD。即如我提到的，犯罪分子会滥用他们所能控制的所有人。他们对谁都漠不关心。

只是有一件事，世界上某些地方的某些犯罪分子会精心编译他们的恶意软件，避免攻击自己所在管辖区的 IP 地址，因为他们不希望自己当地的执法部门也来抓他们，否则他们就麻烦了。所以他们会跳过当地的 IP 地址空间。

当然，他们不能离开自己所在的国家或地区，这算是一件好事。他们相当于将自己监禁在边境以内。好的方面是他们会呆在一个国家或地区中，坏的方面是他们会干很多坏事。

这就是 Avalanche 行动的结果。感谢 Europol 和 FBI 提供内容。这个演示仅用于介绍这个案例。这只是结果。执法部门在 4 个国家和地区抓捕了 5 个人，在 7 个国家和地区开展了 37 项调查行动，在 13 个国家和地区收缴了 39 台服务器，关停了 221 台服务器，在 26 个国家和地区撤下了 64 个 TLD/832,000 个域名，同时还实施了许多受害者缓解措施以及意识提高和威胁防护宣传活动。由此可见，这确实是一场大规模行动。这是件好事，引起了巨大反响。

从 DNS 角度看，WannaCry 挺奇怪的。有趣的是，与其他在普通 TLD（包括 gTLD 和 ccTLD）中利用域名进行命令和控制的常见恶意软件不同的是，WannaCry 主要是通过七个 .onion 域名实施命令和控制。如果你还记得 .onion 的话，.onion 是 IETF 定义的一个专用 TLD，这表示它从来就不在根区，因此 ICANN 无力控制 .onion。因此我们无法撤下与 WannaCry 有关的命令和控制基础设施。

然而，英国的青年研究员 Marcus Hutchins 通过分析代码，获得了 WannaCry 的样本。在分析代码时，他在代码中发现了一个字符串。当然，那个字符串也是硬编码在恶意软件中。他检查那个字符串，发现它没有注册，于是他注册了这个字符串，结果正好遏止了恶意软件的传播。纯属巧合。他也没有想到会发生这样的结果。注册一个域名，就能停止恶意软件传播。

这其中的原理如下：如果我的勒索软件连接到了命令和控制，那么这应该是一种用于规避分析的进程。所幸有这个。WannaCry 停止了传播。

WannaCry 的幕后黑手随即尝试注册第二个字符串，但那个字符串后来也很快被注册了。最后，恶意软件的传播彻底停止。他们跑到其他地方去了。

DNS 滥用是 ICANN 中一个颇具争议的话题。人们各持己见。有些人从安全性和执法部门角度出发，对 WHOIS 的准确性、即将投入运营的 GDPR 的影响，以及 GDPR 在 5 月 25日生效后 WHOIS 将发生什么变化表示担忧。

还有些人对响应时间、反应时间以及何时提交滥用报告等表示担忧。人们对这些方面有着各种不同的担忧。

我们组织必须注意的另一方面意见是，有人认为 ICANN 不应该放弃管理内容的责任。这个意见的根源在于，ICANN 合同中不包含允许撤下盗版内容等方面的条款。这场讨论应该在社群

中进行，而不是由 ICANN 组织来下定论。基本上，这场讨论应该由你们大家来主导。我们会促进这场讨论，但不会参与。

需要注意的是，公共安全工作组是民事及刑事执法部门在 ICANN 组织结构（由各种 ICANN 委员会组成的较大组织）中的官方机构。在组建 PSWG 之前，执法部门社群在 ICANN 组织结构中始终没有一个官方机构，直至美国联邦贸易协会的劳伦 • 卡宾 (Laureen Kapin) 在北京会议上询问前任 CEO 法迪 • 切哈德 (Fadi Chehadé) 是否愿意为执法部门在 ICANN 组织结构中建立一个正式机构。他将问题抛回给了执法部门社群：“请给我一个提案。”然后他们提交了一个提案。我们根据那个提案组建了今天的 PSWG，也就是政府咨询委员会中的一个工作组或小组。他们的从属关系就是这样。

当然，PSWG 旨在向 GAC（政府咨询委员会）以及更大的 ICANN 社群提供建议。他们关注的话题有：DNS 滥用，也就是犯罪分子通过哪些方式出于恶意伤害用户的目的使用域名；GDPR，这个会对可供威胁研究和调查使用的 WHOIS 信息产生一定影响；以及电信级转换 (CGN NAT)，某些 ISP 可能会在短期内使用该技术。某些 ISP 在选择不迁移至 IPv6 时，就会使用这些或其他类似技术。

他们不会迁移至 IPv6，而是创建大型局域网，并为客户分配内部 IP 地址。有些 IP 地址仅供我们平时接触的公共互联网使用。如果分析流量，我们就会发现他们的 IP 地址仅存在于专

用网络中，而绝不会出现在公共互联网中。例如，在我们的公司、家庭网络中，我们的设备分配到的就是这种专用 IP 地址。

这些 ISP 会向客户分配那种专用 IP 地址，无论客户数量是 500、1,000 还是 10,000 人，他们都会用一个公共 IP 地址来创建邻区级专用网络和局域网。这会增加执法部门工作的复杂性，因为当执法部门找上门去向 ISP 送法律文件或者传票，要求他们提供在这一天通过这个 IP 地址发送这种流量的用户的信息时，ISP 可能说：“抱歉，我不知道这到底是谁。这个公共 IP 地址后有 10,000 个用户。”

许多国家和地区都没有明确关于保留、维护和存储流量、登录和注销日志的责任，或者虽然制定了相关法规，但没有确保落实。所以在许多地方，你可以随便登录，注销后便能消失不见，相关数据不会得到保存，没有人知道你曾去过那里，ISP 也不知道你曾去过那里。这就会让事情变得很复杂。PSWG 之前曾讨论过这个问题。快速通量是犯罪分子惯用的一种技术。

这是两个简单示例。并不是只有税务或管制机构的人员、ICANN 合同责任方、更大的网络合同相关方有责任参与反滥用事业。这件事情与很多人有关。哪怕只从 ICANN 合同责任角度来讨论反滥用，我们都可能需要谈上一个小时。

我可以说，注册管理机构确实有责任监控其区域中的安全威胁。我的意思是，他们有责任调查通过自己注册的域名。

如果我是 .carlos TLD 的注册管理机构，我就必须检查所有 .carlos 域名，确定其中是否包含犯罪分子用于实施网络钓鱼、发送垃圾邮件、分发恶意软件、实施命令和控制等的域名，并将相关的统计数据和指标报告给 ICANN。这是注册管理机构必须承担的责任。

另外，我相信注册管理机构还必须提供反滥用联系人信息。我认为注册管理机构在反滥用方面应该做到这个程度才够。

不过，注册服务机构方面的要求更为具体。他们的协议中有更具体的规定。我们对这个协议的非正式叫法是注册服务机构认证协议，即 RAA。

那些更具体的规定是根据现在的 PSWG 提出的 12 项执法部门建议所制定的。PSWG 是在 2012 年哥斯达黎加会议上通过 GAC 成立的，在此之前，我们只有执法部门社群。我想他们应该是在那年会议上提出的那 12 项建议。

董事会根据他们的建议要求员工开始与注册服务机构利益相关方团体进行磋商。磋商是在同一时间的几个月中进行的，最后经各方努力颁布了 2013 年版 RAA，其中包含少量有关反滥用的具体规定。

运营安全性社群中的某些人希望能够制定更明确、更严格的规定，但就这一点而言，执法部门对注册服务机构利益相关方团体与 ICANN 组织商定的协议文本表示认可。

我快速介绍一下，举例而言，这些规定包括注册服务机构必须在收到滥用报告时采取合理行动。当然了，我们向 10 名律师询问什么是“合理的”，可能得到 20 种不同的回答。所以这个问题比较复杂。但 RAA 中现在就是这么规定的。

另外，他们必须提供反滥用联系人。我认为该信息必须发布在网站中，和/或显示在 WHOIS 数据中。可能这些信息通常会显示在 WHOIS 数据中。他们还必须在网站中发布该信息。我不太确定，想必你们也听出来了。反正是要提供这些信息，具体在哪里提供我就不太确定了。

还有一项很有意思的规定，是特定于执法部门的。注册服务机构所在管辖区的执法机构向注册服务机构发送传票时，注册服务机构必须在 24 小时内提供人工回复。记住，两者必须在相同管辖区。这种回复必须是人工的，不能是自动回复。回复不必是“我们已经暂停了那个域名。”也可以简单回复为“收到/我们确认收到了传票。”这就算是有效回复了。

根据协议文本，提供此回复的人必须能够基本上决定将如何处理滥用报告，无论是否会暂停相应域名。

这一规定对于有大量注册服务机构开展运营的管辖区很有帮助，不过有些管辖区内没什么注册服务机构，甚至一个都没有。所以这一规定的效力将因具体管辖区而异。

隐私和代理服务提供商；大家还记得吗，注册人可以通过这些服务在其域名的 WHOIS 输出中显示其他人的信息，而不提供

自己的信息。如果我有一个网站，但我不希望显示我自己的姓名、地址或电子邮件，那么注册服务机构控制的那些隐私和代理服务提供商就必须提供他们的反滥用联系人信息。

我觉得就是这样了。这些就是我们要讨论的话题。内容很多。我刚才说过，DNS 滥用在某些情况下很明显，如果你看到某个域名被用于实施僵尸网络的命令和控制，那么很明显这是 DNS 滥用。当你发现这种域名时，你可以进行各种技术分析，没有人能否认实际的技术和科学证据，因为事实就是如此。但在另外一些情况下，它会更复杂。

所以这个话题仍有待我们继续讨论，有待社群继续深入探讨。

刚才开场时我忘了说一件事，我是安全、稳定与弹性工作组的一名董事，负责安全、稳定与弹性合作事务。我们隶属 CTO 办公室。我们会与运营和安全性社群以及执法部门进行大量互动。

我们会调查很多方面。我们会尝试让他们进一步融入 ICANN 组织结构。我们希望帮助他们理解我们社群中正在进行的所有讨论。就在几周前，一位域名行业代表应我们邀请参加了一场安全性大会。那是信息传递、恶意软件和移动反滥用工作组。那是约坦 • 弗雷克斯 (Jonathan Frakes)，域名协会执行董事。他参与活动很积极。

那是我们做的一项工作。我们会通过互动尝试撮合过去历来针锋相对的群体，我们尝试让他们能够彼此理解。如果他们他们能够理解对方的故事，或许便能够在此基础上达成某些一致。

我们还为执法部门提供培训。如果大家还记得的话，ICANN 的职责之一便是帮助维护域名系统的安全、稳定与弹性。所以执法部门在调查僵尸网络或者恶意软件分发事件时，必须知道自己在做什么。他们需要了解 DNS 的运作原理。我们帮助他们从这个角度理解域名系统，从而他们能够更好地帮助维护系统的 SSR，也就是安全、稳定与弹性。

我觉得就是这样了。如果大家有问题，请自由提问。

凯西 • 彼得森： 提醒一下，请报出你们的姓名和附属机构，如果你有组织的话。

马西 • 苏尔摩 (MARSY SURMO)： 大家好，我是来自印度的马西 • 苏尔摩。[听不清楚] 问题：ICANN 是否已经为 DNS 的实施或运营制定一些基本的安全性标准？能够通过其他方式维护吗？它也许只是一个可操作设备，谈不上任何安全性。所有类型的滥用都有可能发生。那就只能进行事后分析了。所以我想确认一下：有没有可能在运营 DNS 之前制定最低的基本安全性标准？

卡洛斯 • 奥法瑞兹： 对于这个问题，我建议你查阅 DNS-OARC（也就是 DNS 运营商社群）发布的文档。当然，毋庸置疑的是，IETF 标准中的某些安全性规定也与 DNS 有关。然后我还建议你查阅 M3AAWG 的文档。大约在一年半之前，他们更新了一份文档，我不记得文档名称了。你搜索“M3AAWG DNS 威胁”就可以找到它。我很确定。其中也提供了一些有用的信息。

这些社群或工作组已经着手制定你刚才所说的文档或标准。

马西 • 苏尔摩： 这只是一个指导方针。我们能否 [听不清楚] 之前 [听不清楚] 这些设备，实施这些最低安全性标准？

卡洛斯 • 奥法瑞兹： 这个无法强制实施。任何人都可以搭建、启动和运营 DNS 服务器。世界上任何一个人都可以。我们无法采取强制措施。这是在技术上无法阻止的事情。没有任何规则，没有任何约束，任何人都可以随心所欲地做。这是自愿性质的，因此也会带来不确定性。

对于你说的问题，就其自愿性质而言，技术社群多年前就已经制定了相关标准和行为准则，例如他们在 1997 年便针对过滤恶意 IP 地址制定了标准。你搜索 BCP 38 或 BCP 84，就可以找到那些 20 年前的最佳实践。不过，由于它的自愿性质，那些标准没有得到广泛实施，或者说实施范围没有达到你所设想那般广泛。它是自愿的。

还有谁有问题吗？

请发言。

哈鲁 • 阿 • 哈桑
(HARU AL HASSAN)： 实际上 -

卡洛斯 • 奥法瑞兹： 请报一下姓名和附属机构。

哈鲁 • 阿 • 哈桑： 我叫哈鲁 • 阿 • 哈桑，来自尼日利亚。作为发展中国家，我们面临的挑战是：我们如何为执法机构提供培训，以便应对犯罪分子的挑战？你刚才介绍了犯罪分子可能采用许多手段来攻击 DNS 和进行投毒，我们如何针对这些为执法机构提供培训？

卡洛斯 • 奥法瑞兹： 我觉得你们可以与非洲的 ICANN 合作部员工取得联系。应该就是皮埃尔。不知道你和他是不是已经认识了。你可以将你的担忧跟他说说。

然后，皮埃尔将与我们的 SSR 团队协调，安排你们的执法机构参加 DNS 反滥用培训。所以，我的建议就是你去找皮埃尔，这个担忧应该很普遍。

请发言。

布伦特 • 凯里
(BRENT CAREY)： 我是布伦特 • 凯里，来自 .nz。我想问一下你们有没有提供各种互联网和管辖区的链接？上周我在渥太华参加了一个会议，了解了一些域名系统面临的压力。很显然，现在各种基础设施滥用、注册滥用以及内容滥用可能同时出现。所以我希望你们会提供一些链接。

卡洛斯 • 奥法瑞兹： 我们还没有准备这类的链接。回头准备吧。现在还没有。你说的这个事情我知道，当时我们曾试图在渥太华组织一个论坛。我的一些 ICANN 同事去参加会议了。

布伦特 • 凯里： 因为执法部门显然没有来参加会议，所以我有此一问。

卡洛斯 • 奥法瑞兹： 好的。我不知道。也许这个问题应该转交给 PSWG。谢谢。

布伦特 • 凯里： 谢谢。

卡洛斯 • 奥法瑞兹： 好的。还有人要提问。

男性发言人（姓名不详）： 我附和一下 [听不清楚] 说我们没有建立稳健的机制 [听不清楚] 这个 WHOIS 的 GDPR。另外，我们没法控制这些安全性问题。很难解决，但以后可能会这样。

卡洛斯 • 奥法瑞兹： 什么问题很难解决？

男性发言人（姓名不详）： 一方面，我们没有真实的 WHOIS 信息。在这个 GDPR 的构架中，我们可能无法知道我们面对的是什么人，以及我们将去往哪里。

卡洛斯 • 奥法瑞兹： 对的。

男性发言人（姓名不详）： 第二，我们的 DNS 不够安全。我们没法掌控它。所以我们无法控制我们要去往哪里，也不知道对方的真实身份。

卡洛斯 • 奥法瑞兹： 等一下。关于你的问题，我建议你通过 ICANN 组织内的电话会议参加讨论并提供反馈。CEO 在稍后一般都会通过电话会议向大家征求反馈意见。你一定要参加那个电话会议，你这个意见适合在那边说。你的意见会得到关注。我不是开玩笑。他们会认真听取你的意见。你可以在那边表述你的担忧。你这个问题适合在那边说。

他们会专门举行一些这方面的会议。今天我们这个会议并非唯一有关 DNS 滥用的活动。大家请记住这一点。如果时间能够倒转，你昨天 11:30 可以参加 PSWG 消息更新会议，明天上午 8:30 会举行一场 GAC PSWG 会议。我建议你参加这些会议。

我个人比较倾向于参加 GDPR 会议，因为它也会讨论这些问题。但两场会议都很有意思。

这样你就能了解域名行业正在实施哪些措施来保证域名的健康。了解他们的活动很重要，他们做的事情都很有意思。

DAAR 是我们团队开发的一个工具。它可以提供有关恶意注册的信息，以及不同领域的恶意注册汇总数据。这些也很有意思。我不准备对此做详细介绍，因为我希望你们都去参加那个会议。大家都去吧。很有意思的。

好的。非常感谢大家参加这个会议。

凯西 • 彼得森： 提醒一下：本场会议的演示幻灯片已经发布在公开时间表上。几天后，我们还会添加抄录脚本和会议媒体资料。这样大家就能随时查阅本场会议的内容。

非常感谢。我们将在 3:30 举行下一场工作原理会议，主题是“互联网网络”。不是 3:15，而是 3:30。抱歉，下一场工作原理会议要延迟一下了。“互联网网络”会议将集中介绍 IPv4 和 IPv6 协议。

现在大家可以休息一下，四处走走，喝杯咖啡，然后请准时回来开会。谢谢。

[会议记录结束]