对因新冠肺炎疫情相关封闭措施给 IMRS 流量带来的影响的分析

ICANN 首席技术官办公室

罗伊·阿伦兹 (Roy Arends)
OCTO-008
2020-04-15

ICANN

目录

本文档是 OCTO 文档系列的一部分。要查看 OCTO 系列文档，请参阅 https://www.icann.org/resources/pages/octo-publications-2019-05-24-en。关于这些文档，如果您有任何问题或建议，请发送至 octo@icann.org。

执行摘要

新冠肺炎疫情期间采取的封闭措施和学校停课，预计对 ICANN 管理的根服务器 (IMRS) 域名系统 (DNS) 流量产生的影响虽然有限，但仍然十分明显。ICANN 的首席技术官办公室 (OCTO) 针对法国在全国范围采取封闭措施对法国境内四个 IMRS 实例的流量及流量组成变化所造成的影响进行了分析。

欧洲网络协调中心 (RIPE NCC) Atlas 探测器显示，法国 IMRS 实例的流量大部分源自法国。法国从 2020 年 3 月 17 日（2020 年第 12 周）开始实施封闭措施。第 12 周的流量统计数据显示，与前 6 周的平均值相比，这一周的流量增加了 28%。我们将第 6 周和第 12 周的流量数据进行了比较分析，同时还对以下类别的数据进行了比较：

- 对现有顶级域 (TLD) 的查询
- 源自基于 Chromium 的浏览器的查询
- 对长 TLD 的查询
- 对常用 TLD（.home、.lan、.corp 和 .local）的查询
- 所有其他查询

大多数类别的流量都有所增加，推动了总体流量的增长。源自 Chromium 浏览器的这一类查询量最大，占所有收到的查询请求的大约三分之一。一些类别的查询量增速快于其他类别。最大增幅来自对四类不存在的常用 TLD（.home、.lan、.corp 和 .local）的查询。这可能是由于人们更多地开展居家办公，因为通常情况下，员工在办公室使用一组解析器工作，这些解析器知道如何响应 .corp、.lan 和 .local 域。但是现在员工居家办公，位置更加分散，使用的解析器可能不知道如何响应这些域。此外，这也可以解释 .home 查询增加的原因：越来越多的人居家使用互联网。

从国家/地区层面来看，在全国范围采取封闭措施对 IMRS 实例中的 DNS 流量产生的影响虽然有限，但也十分明显。可以观察到 DNS 总体流量有所增加，与此同时，没有出现任何问题这一事实表明，在远程办公和居家上网增加的这段期间，DNS 架构非常适合扩展。

1 简介

在全国范围采取封闭措施、活动限制以及学校停课，预计对 IMRS 实例中的 DNS 流量产生的影响虽然有限，但仍然十分明显。总体来说，在 IMRS 中看到的大部分 DNS 流量来自解析器，这些解析器代表客户端，例如，手机、平板电脑、个人计算机（笔记本电脑和台式机），游戏机等提交 DNS 请求。这些解析器能够临时缓存信息，从而减轻根服务器上的负载。例如，如果解析器缓存了关于 .com 域名空间的域名服务器信息，则它无需联系根服务器以获取有关 example.com 的信息，只需查询 .com 域名服务器即可。

截至编写本报告时（2020 年 3 月 31 日），IMRS 包含 167 个实例，这些实例分布在 83 个国家/地区。此次研究重点关注位于法国的四个 IMRS 实例。之所以重点关注位于法国的这些实例，是因为法国政府紧急陆续要求学校停课，实施活动限制，并在全国范围采取封闭措施。3 月 12 日，政府宣布全国的大中小学从 3 月 16 日星期一开始停课。3 月 13 日，政府严禁 100 人以上的集

会。3 月 14 日，政府下令关闭所有非必要的公共场所，包括餐馆、咖啡馆、电影院和迪斯科舞厅。3 月 16 日，政府下令自 3 月 17 日开始实行全国范围封闭。

到达 IMRS 服务器的流量源自各个地区，不一定与所查询的实例位于同一国家/地区。通过将 RIPE Atlas[1] 探测器作为解析器客户端的代理，我们可以清楚地看到哪些探测器使用了目前位于法国的四个 IMRS 实例。

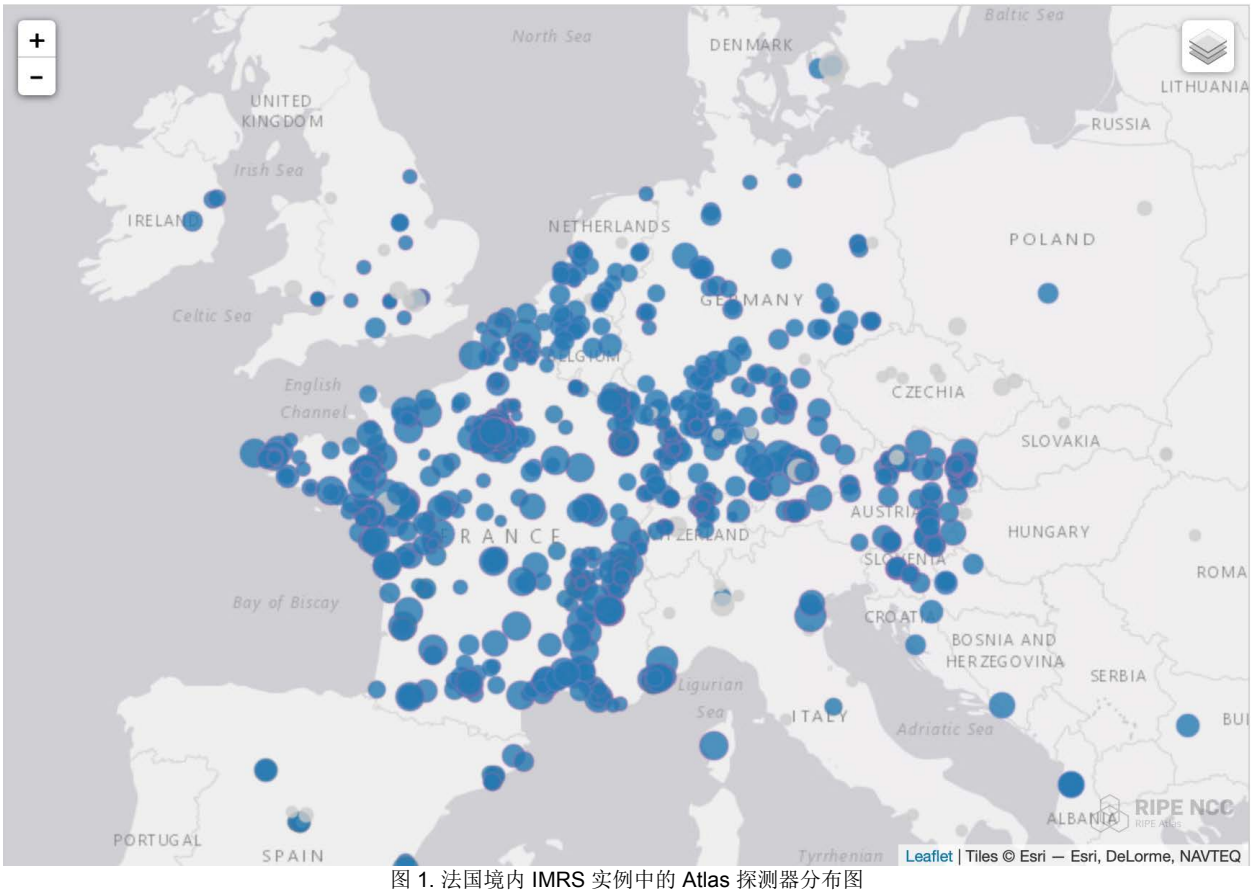

图 1. 法国境内 IMRS 实例中的 Atlas 探测器分布图

如图 1 所示，虽然有相当多位于法国境外的探测器收到了来自上述 IMRS 实例的响应，但是法国境内 IMRS 实例的大部分流量还是源自法国。

[1] RIPE Atlas 是一个开放式全球分布互联网测量平台，它由数以千计的测量设备组成，这些设备实时监测互联网连接情况。

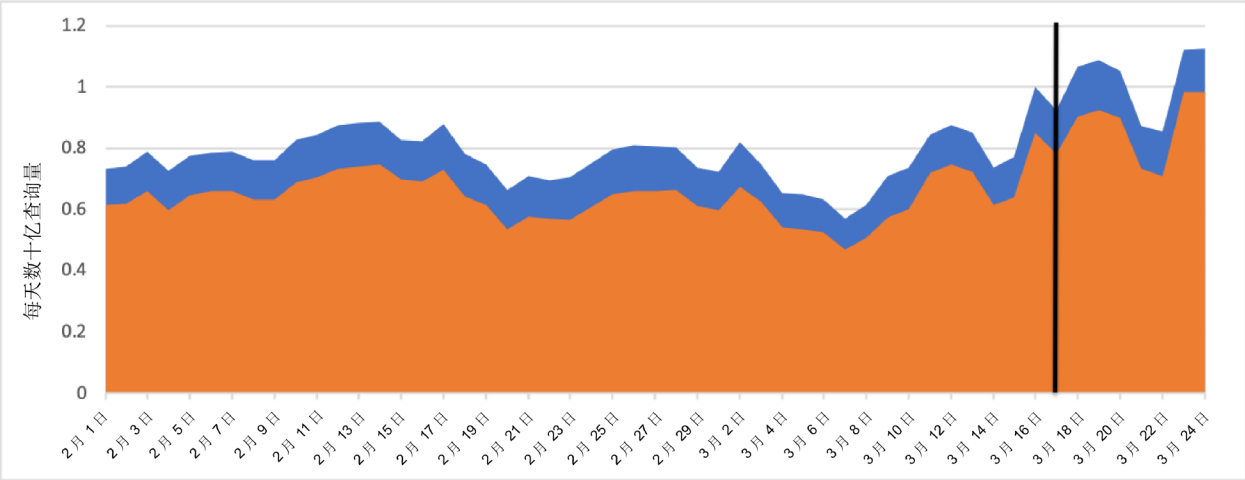

图 2. 法国境内 4 个 IMRS 实例中观察到的每日查询量（蓝色）和每日 NXDOMAIN 响应量（橙色）。黑色垂直线表示从 3 月 17 日开始。

如图 2 所示，流量自 3 月 16 日之后有所增加。为了解导致流量增加的原因，我们对流量的构成进行了研究。我们将对 3 月 16 日之前和之后的流量构成进行比较，看看流量构成变化是否与封闭有关。

2 方法

我们将比较两周的流量，即，2 月的第一周（第 6 周，从 2 月 3 日开始）与封闭后的第一周（第 12 周，从 3 月 16 日开始）。然后，我们会对部分流量进行分类，看看哪类流量变化最明显。

2.1 分类

根据所查询的 TLD，流量分为以下几个类别：

- **现有域名**：对当前从根区授权的 TLD 的查询
- **Chrome**：对长度在 7 到 15 个字符之间的不存在的 TLD 的查询
- **Jumbo**：对长度超过 15 个字符的不存在的 TLD 的查询
- **.home**：对以 .home 结尾的域的查询
- **.lan**：对以 .lan 结尾的域的查询
- **.local**：对以 .local 结尾的域的查询
- **.corp**：对以 .corp 结尾的域的查询
- **其他**：对所有其他域的查询

2.1.1 Chrome 查询

Chromium Web 浏览器及衍生产品（例如 Google Chrome、最新版本的 Microsoft Edge、Amazon Silk 以及 Opera 的 Web 浏览器）会发出三个带有随机标签的 DNS 请求，以检测本地网络上使用的解析器是否会重定向不存在的域，例如，对于不存在的域的查询，是否会返回

“helper（助手）”搜索网站地址。标签由随机字符组成，长度在 7 到 15 个字符之间。[2]由于查询的域是随机的，所以接收解析器不会对其进行缓存，而是会向根服务器发出查询。在没有重定向的网络中，该随机查询的预期响应是一个 NXDOMAIN 错误代码。

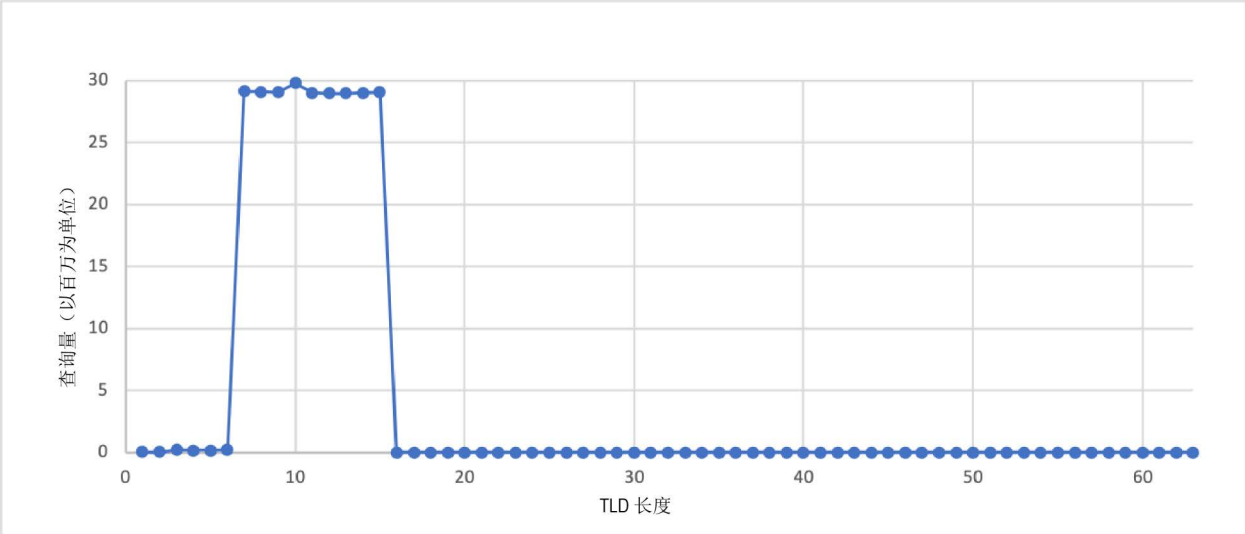

图 3. 按 TLD 长度划分的对不存在的 TLD 查询数量直方图。

图 3 中的直方图显示了从 3 月 19 日起的数据，这些数据按 TLD 长度显示了查询频率分布情况。这些查询大部分是针对长度在 7 到 15 个字符范围内的域名。图 5 显示了这些 Chrome 查询量占所有不存在域查询总量的 28%。

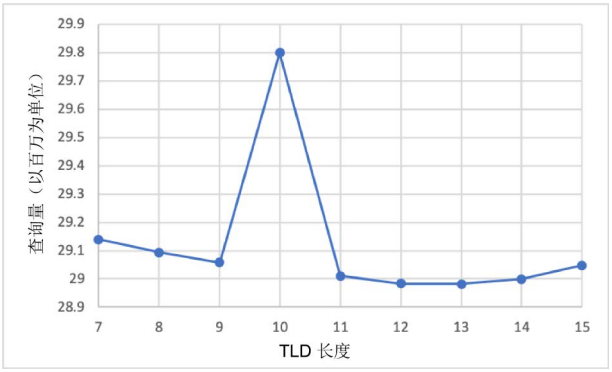

图 4. 按 TLD 长度划分的对不存在的 TLD 查询数量详细直方图。

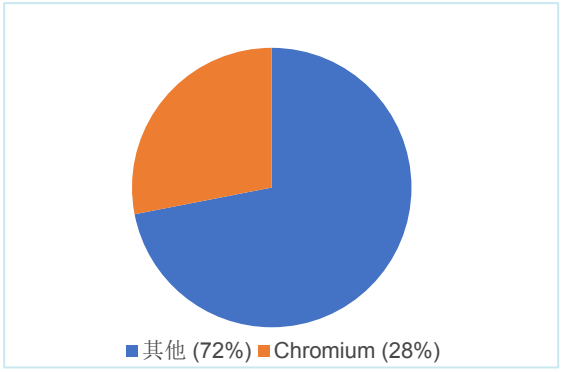

图 5. Chromium 查询量占所有不存在的域查询总量的百分比。

除了长度为 10 个字符的 TLD 之外，长度在 7 到 15 个字符的 TLD 的查询量分布相当均匀。对长度为 10 个字符的标签查询量异常，可能是因为旧版本的 Chrome 发布了长度为 10 个字符的随机域。[3]

[2] “我们将生成一个 7 到 15 个字符的随机主机名。
"https://chromium.googlesource.com/chromium/src/+/master/chrome/browser/intranet_redirect_detector.cc#150

[3] “改变 DNS 的长度会劫持检测域名。”
https://src.chromium.org/viewvc/chrome?view=revision&revision=249013

2.1.2 Jumbo 查询

这些是针对长度超过 15 个字符的不存在的 TLD 的查询。我们尚不知晓这些查询的来源或原因。

2.1.3 常见的不存在的 TLD

有一些常见标签没有在根目录下授权，并且不存在于互联网的公共 DNS 域名空间中。在这些不存在的 TLD 中最常见的是 .home、.lan、.corp 和 .local。之所以将这些 TLD 单独分类，是因为在我们的研究过程中，它们的查询量都在增加。

2.1.4 其他

这个类别囊括了所有不能归类到前面所述任何类别的查询。

3 观察结果

在第 6 周到第 11 周期间，法国四个 IMRS 实例平均每周收到 54 亿个 DNS 查询请求（见图 6）。这四个实例在第 12 周收到了 69 亿个 DNS 查询请求。这表明，到达这四个 IMRS 节点的流量增加了 28%。

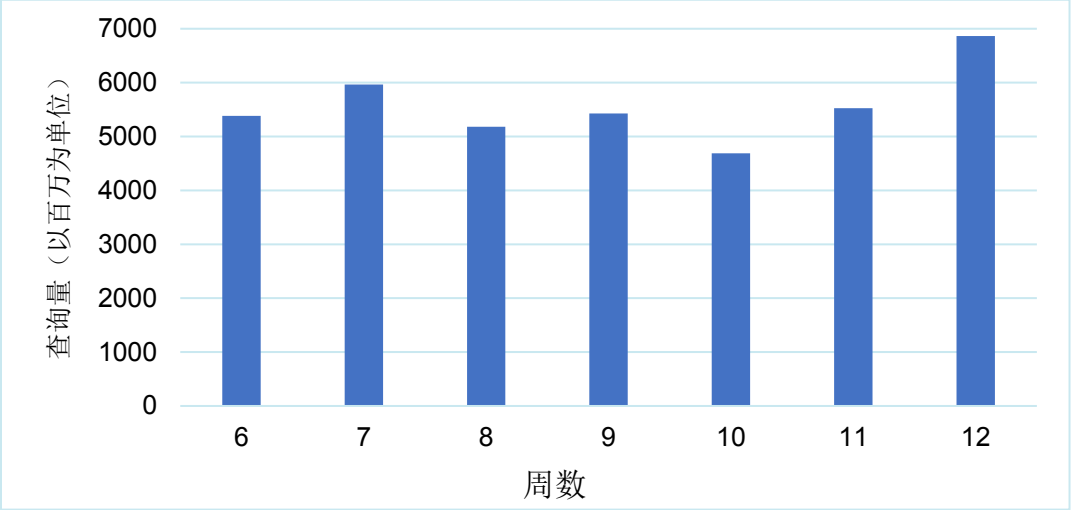

图 6：从第 6 周到第 12 周，法国境内 4 个实例上的每周查询量。

我们确实注意到了一些异常情况，例如，短时间的流量暴增或该时段内因实例维护而中断，但这些异常情况往往是短暂的，我们认为不会显著影响总体流量。由于流量在一周当中不断累积，因此我们也采取了其他一些流量模式，例如每日模式或周末模式。我们没有发现在这段时间内有任何其他变化或事件显著影响 DNS 查询量。

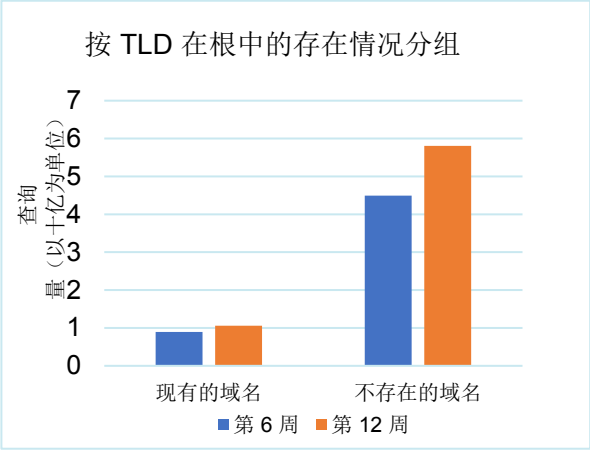

图 7：第 6 周和第 12 周对现有 TLD 和不存在的 TLD 的查询流量

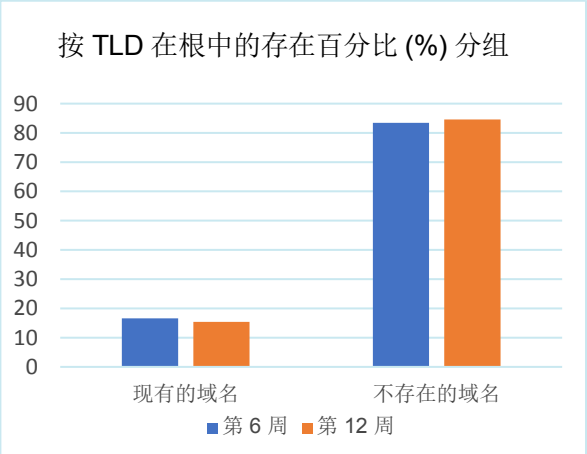

图 8：第 6 周和第 12 周对现有 TLD 和不存在的 TLD 的查询流量占这两周查询总量的百分比

图 7 显示了对现有域和不存在的域的查询量在绝对数量上的差异。这两组的查询量都有增加。图 8 显示流量的构成也出现了细微变化，因为与对不存在的域的查询量相比，对现有 TLD 的查询百分比有所下降。流量增加主要是对不存在的域的查询量增加。

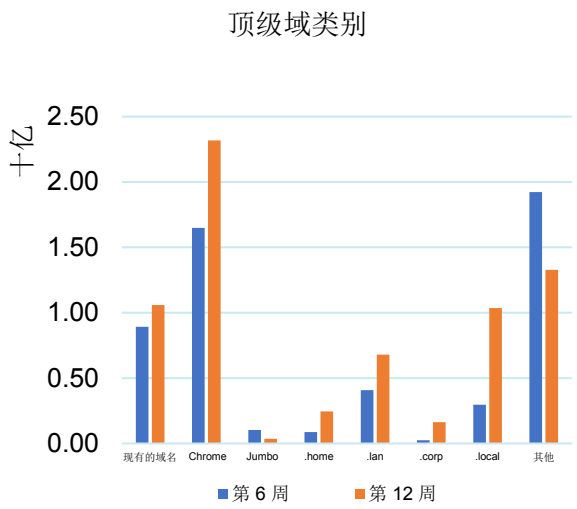

图 9：第 6 周和第 12 周不同类别流量按绝对数量进行分类对比。

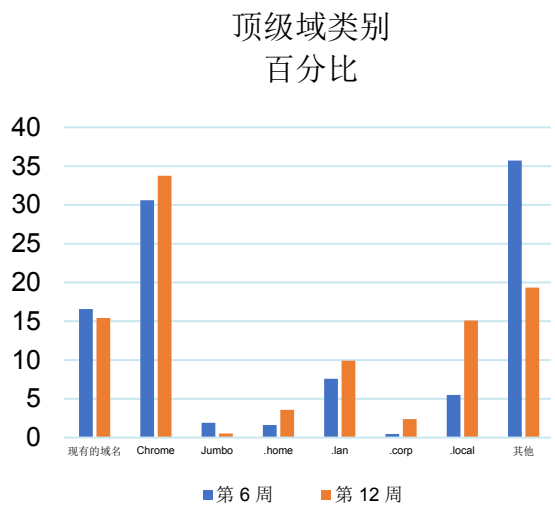

图 10：第 6 周和第 12 周不同类别流量按占总量百分比进行分类对比。

3.1 Chromium 查询

我们观察到，第 6 周收到的请求中有 31% 属于 Chromium DNS 查询请求，而第 12 周收到的请求中有 34% 属于 Chromium DNS 查询请求。这在总流量中占据重要部分。采取封闭措施后，查询请求总数增加了 28%，而其中 Chromium 查询请求增加了 41%。这一增长很可能是由于人们在遵循居家隔离的强制要求期间，更加频繁地通过设备上网。

由于 Chromium 会重定向 DNS 检测查询，因此，当更多使用基于 Chromium 浏览器的设备上网时，流量中对长度介于 7 到 15 个字符之间的随机字符串的 DNS 请求率会更高。请注意，Chromium DNS 查询请求的增长率与总体流量增长率不同。这表明总体流量构成略有变化。其他类别查询的增长率高于 Chromium 查询增长率。

Chromium 查询是导致根服务器查询的最大单一因素。其他 IMRS 实例通常显示所有传入查询中超过 50% 源自 Chromium。这些查询的目的是检查强制网络门户是否由 Chromium 提供支持。设置根服务器通常是指配置根服务器总体负载，以满足扩展需求。虽然 Chromium 可以免费进行这些查询，但根服务器实例的设置成本却不是免费的。我们已将这个问题告知 Google，但仍未得到解决。[4]

3.2 Jumbo 查询

我们观察到，针对长 TLD 域（超过 15 个字符）的查询请求数量有所减少。我们尚未调查这类流量减少的原因。

3.3 常见的不存在的 TLD

查询数量有所增加的四种最常见的不存在的 TLD 是 .corp、.home、.lan 和 .local。其中 .corp、.lan 和 .local 的查询量增长最为显著。这可能是因为人们更多地居家办公。通常情况下，员工在办公室里使用一组解析器，这些解析器知道如何响应 .corp、.lan 和 .local 域。但是现在员工居家办公，分布位置更加分散，使用的解析器可能不知道如何响应这些域。此外，这也可以解释 .home 查询增加的原因：越来越多的人居家使用互联网。

4 结论

从国家/地区层面来看，在全国范围采取封闭措施以遏制全球疫情对 IMRS 实例中的 DNS 流量产生的影响虽然有限，但也十分明显。可以观察到 DNS 总体流量有所增加。没有出现任何问题这一事实表明，在远程办公和居家上网增加的这段期间，DNS 架构非常适合扩展。

作者：阿迪尔·阿科普罗根 (Adiel Akplogan)、罗伊·阿伦兹 (Roy Arends)、戴维·康纳德 (David Conrad)、阿兰·杜朗德 (Alain Durand)、保罗·霍夫曼 (Paul Hoffman)、大卫·休伯曼 (David Huberman)、麦特·拉森 (Matt Larson)、西昂·劳埃德 (Sion Lloyd)、特里·曼德尔森 (Terry Manderson)、戴维·索尔特罗 (David Soltero)、萨马内·塔杰扎德赫克霍伯 (Samaneh Tajalizadehkhoob)、莫里西奥·维尔加拉·埃雷切 (Mauricio Vergara Ereche)。

[4] 由于内部网重定向检测器使用的三个随机探测器没有 TLD，因此会到达根服务器。
https://bugs.chromium.org/p/chromium/issues/detail?id=946450&q=intranet%20redirect&can=2