Análisis de los efectos de los confinamientos relacionados con la COVID-19 en el tráfico de IMRS

Oficina del Director de Tecnologías de la ICANN

Roy Arends
OCTO-008
15 de abril de 2020

ICANN

ÍNDICE

El presente documento forma parte de la serie de documentos de la OCTO. Consulte https://www.icann.org/resources/pages/octo-publications-2019-05-24-en para obtener una lista de los documentos de la serie. Si tiene preguntas o sugerencias sobre cualquiera de estos documentos, escríbanos a octo@icann.org.

Resumen Ejecutivo

Se espera que las restricciones durante los confinamientos relacionados con la COVID-19 y los cierres de escuelas tengan un efecto limitado, aunque notable, en el tráfico del Sistema de Nombres de Dominio (DNS) en los Servidores Raíz Gestionados por la ICANN (IMRS). La Oficina del Director de Tecnologías (OCTO) de la ICANN ha estudiado el impacto de un confinamiento a nivel nacional en Francia sobre los cambios en el volumen y la composición del tráfico hacia las cuatro instancias de IMRS en Francia.

Las sondas Atlas del Réseaux IP Européens Network Coordination Centre (RIPE NCC) mostraron que el tráfico de las instancias de IMRS de Francia se originaba principalmente en Francia. El confinamiento en Francia comenzó el 17 de marzo de 2020 (semana 12 de 2020). Las estadísticas de tráfico de esta semana mostraron un aumento del 28 % en comparación con el promedio de las 6 semanas anteriores. Se realizó un análisis comparativo entre la semana 6 y la semana 12, y se compararon las siguientes categorías:

- Consultas de dominios de alto nivel (TLD) existentes
- Consultas que se originan desde navegadores basados en Chromium
- Consultas de TLD largos
- Consultas de TLD populares (.home, .lan, .corp y .local)
- Todas las demás consultas

En la mayoría de las categorías se registró un aumento del tráfico, lo que contribuyó al aumento general. La categoría de consultas de mayor tamaño se originó en los navegadores Chromium, que se mantuvieron en alrededor de un tercio de todas las solicitudes recibidas. Algunas categorías registraron un crecimiento más rápido que otras. El aumento con mayor porcentaje provino de las cuatro categorías de los TLD inexistentes populares (.corp, .home, .lan y .local). Esto se debe probablemente a que la gente trabaja más desde la casa, dado que normalmente los trabajadores se congregan en las oficinas y utilizan un conjunto de resolutores que comprenden cómo responder a los dominios .corp, .lan y .local. Ahora, están más dispersos y trabajan desde la casa utilizando resolutores que pueden no entender cómo responder a estos dominios. Esto también explicaría el aumento de las consultas en .home: más gente utiliza Internet más a menudo desde sus casas.

Los efectos de los confinamientos a nivel nacional han tenido un efecto limitado, aunque notable, en el tráfico del DNS en las instancias de IMRS cuando se observaron a nivel de país. Este aumento del tráfico del DNS puede observarse en general y el hecho de que no haya surgido ningún problema sugiere que la arquitectura del DNS se adapta bien a la escala durante el trabajo a distancia y el aumento del uso en el hogar.

1 Introducción

Se espera que los efectos de los confinamientos a nivel nacional, las restricciones de las actividades y los cierres de escuelas tengan un efecto limitado, aunque detectable, en el tráfico del DNS en los IMRS. En términos generales, el grueso del tráfico del DNS que se ve en los IMRS proviene de los resolutores que presentan solicitudes de DNS en nombre de clientes como teléfonos móviles, tabletas, computadoras personales (portátiles y de escritorio), consolas de juegos, etc. Estos resolutores tienen la capacidad de almacenar temporalmente en

caché la información, lo que reduce la carga de los servidores raíz. Por ejemplo, cuando un resolutor ha almacenado en caché información sobre los servidores de nombres del espacio de nombres .com, no necesita ponerse en contacto con los servidores raíz para obtener información sobre ejemplo.com, solo necesita preguntar a los servidores de nombres .com.

En el momento de redactar el presente documento (31 de marzo de 2020), los IMRS constan de 167 instancias ubicadas en 83 países. Este estudio se centra en las cuatro instancias de IMRS en Francia. El motivo del enfoque en estas instancias es que, en Francia, el gobierno anunció, en una rápida sucesión, el cierre de escuelas, la restricción de las actividades y el confinamiento en todo el territorio nacional. El 12 de marzo, el gobierno anunció que las escuelas y universidades cerrarían a partir del lunes 16 de marzo. El 13 de marzo se prohibieron las reuniones de más de 100 personas. El 14 de marzo se ordenó el cierre de todos los lugares públicos no esenciales, incluidos restaurantes, cafés, cines y discotecas. El 16 de marzo, se ordenó un confinamiento nacional que comenzó al día siguiente.

El tráfico hacia los IMRS se origina en una amplia variedad de fuentes que no necesariamente residen en el mismo país que las instancias consultadas. Mediante el uso de las sondas RIPE Atlas[1] como un proxy para los clientes de resolutores, podemos visualizar qué sondas individuales usan las cuatro instancias de IMRS actualmente ubicadas en Francia.

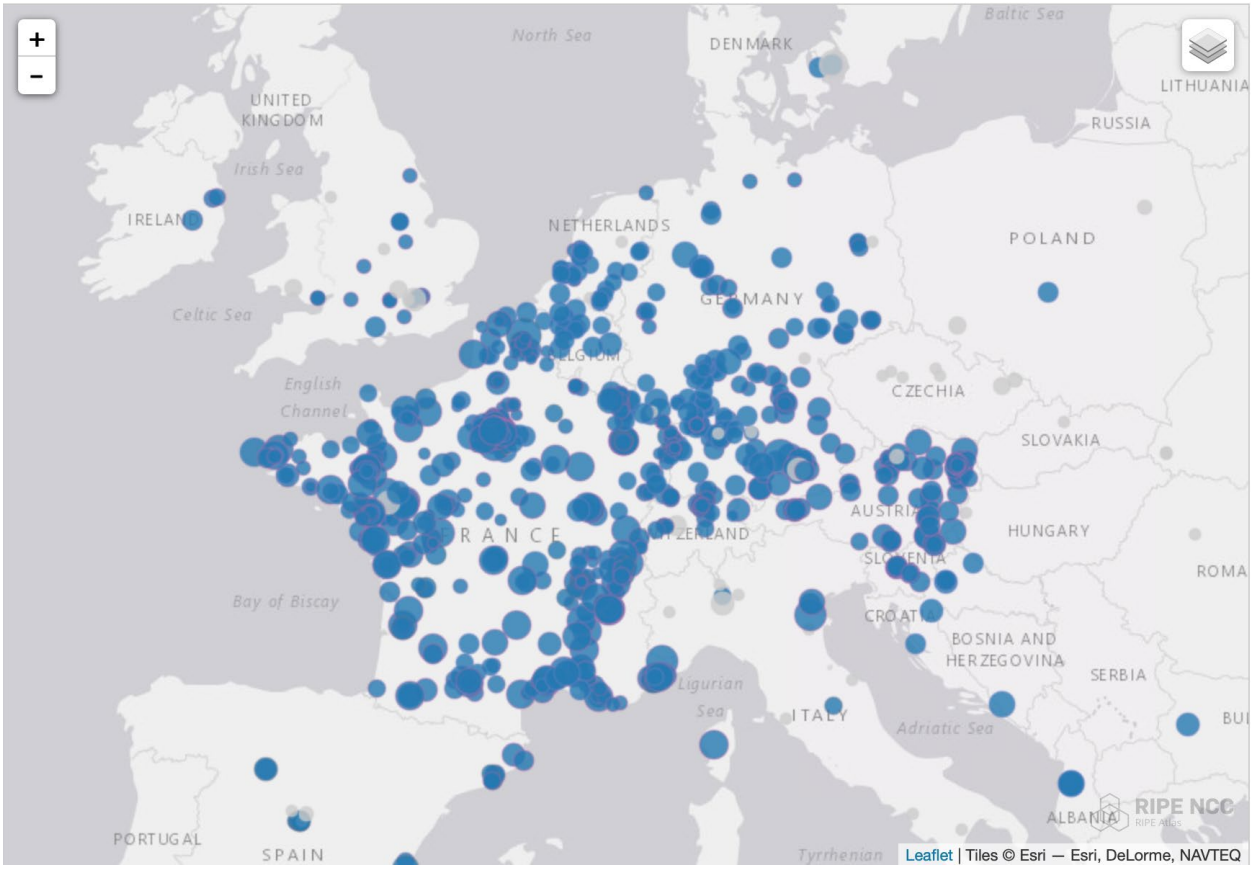

Figura 1: distribución de sondas de Atlas en los colectores de instancias de IMRS situados en Francia

[1] RRIPE Atlas es una plataforma de medición global, abierta y distribuida de Internet, compuesta por miles de dispositivos de medición que miden la conectividad de Internet en tiempo real.

Como se observa en la Figura 1, si bien hay una cantidad considerable de sondas ubicadas fuera de Francia que han visto una respuesta de las instancias de IMRS mencionadas anteriormente, una cantidad significativa de tráfico para las instancias de IMRS en Francia se origina en Francia.

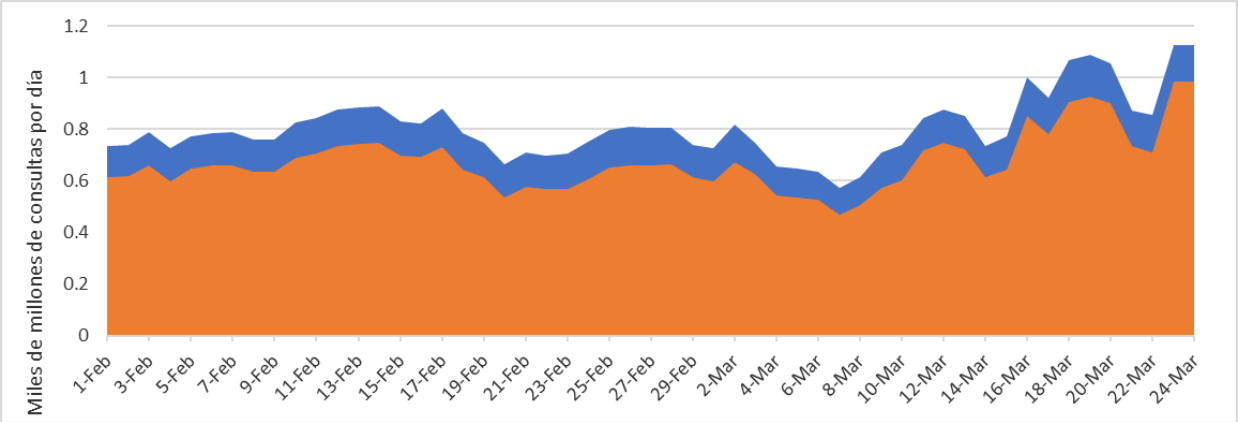

Figura 2: volumen diario de consultas (azul) y volumen diario de respuestas de NXDOMAIN (naranja) observados en las 4 instancias de IMRS en Francia. La línea vertical negra indica el inicio del 17 de marzo.

Como se muestra en la Figura 2, hubo un aumento en el volumen de tráfico después del 16 de marzo. Para comprender qué impulsó este aumento, examinamos la composición del tráfico. Compararemos la composición antes y después del 16 de marzo para ver si podemos correlacionar los cambios en la composición con los confinamientos.

2 Metodología

Compararemos dos semanas de tráfico. La primera semana de febrero (semana 6, a partir del 3 de febrero) frente a la semana del 16 de marzo (semana 12) que fue la primera semana del confinamiento. Posteriormente, clasificaremos partes de ese tráfico y mostraremos qué clasificación tiene los cambios más significativos.

2.1 Clasificación

El tráfico se agrupa en varias categorías en función del TLD por el cual se consulta:

- **Existentes**: consultas de los TLD que están actualmente delegados de la zona raíz
- **Chrome**: consultas de TLD inexistentes con una longitud entre 7 y 15 caracteres
- **Jumbo**: consultas de TLD inexistentes con una longitud superior a 15 caracteres
- **.home**: consultas de dominios que terminan en .home
- **.lan**: consultas de dominios que terminan en .lan
- **.local**: consultas de dominios que terminan en .local
- **.corp**: consultas de dominios que terminan en .corp
- **Otros**: consultas de todos los otros dominios

2.1.1 Consultas Chrome

El navegador web Chromium y sus derivados (como Google Chrome, las versiones recientes de Microsoft Edge, Amazon Silk y el navegador web de Opera) emiten tres solicitudes de DNS con una etiqueta aleatoria para detectar si el resolutor en uso en la red local redirige dominios inexistentes, por ejemplo, si la consulta devuelve la dirección de un sitio web de búsqueda de "ayuda" para dominios que no existen. La etiqueta consiste en letras aleatorias y tiene entre 7 y 15 caracteres de largo.[2] Dado que el dominio consultado es aleatorio, el resolutor receptor no lo tendrá almacenado en caché y emitirá una consulta a un servidor raíz. En las redes sin redireccionamiento, la respuesta esperada de esa consulta aleatoria sería un código de error NXDOMAIN.

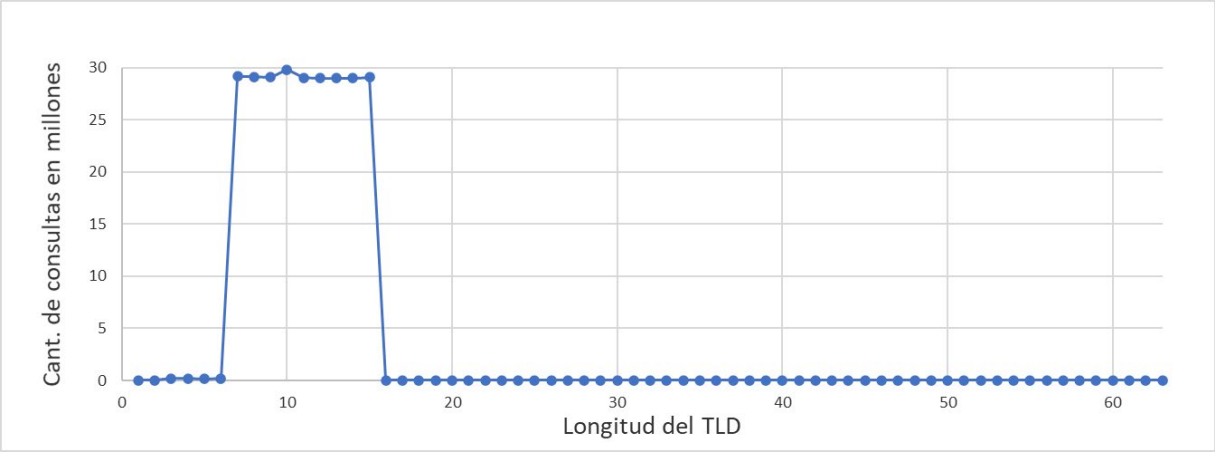

Figura 3: histograma de cantidad de consultas de TLD inexistentes por longitud de TLD.

El histograma de la figura 3, que muestra los datos del 19 de marzo, muestra la distribución de frecuencia de las consultas por longitud del TLD. La mayor parte de estas consultas son de nombres de dominio de entre 7 y 15 caracteres. La figura 5 muestra que estas consultas Chrome constituyen el 28 % de todas las consultas de dominios inexistentes.

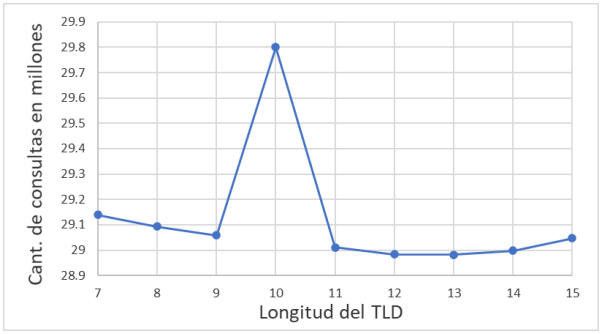

Figura 4: detalle del histograma de cantidad de consultas de TLD inexistentes por longitud de TLD.

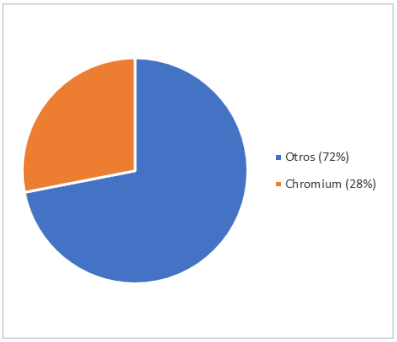

Figura 5: cantidad de consultas de Chromium sobre todas las consultas de dominios inexistentes.

[2] "Generamos un nombre de host aleatorio con una longitud entre 7 y 15 caracteres". https://chromium.googlesource.com/chromium/src/+/master/chrome/browser/intranet_redirect_detector.cc#150

Aparte de los TLD de 10 caracteres, la distribución entre los TLD de entre 7 y 15 caracteres es bastante uniforme. La anomalía de las etiquetas de 10 caracteres se puede atribuir a versiones anteriores de Chrome que emitían dominios aleatorios de 10 caracteres.[3]

2.1.2 Consultas Jumbo

Estas son consultas de TLD inexistentes con una longitud superior a 15 caracteres. Desconocemos los orígenes o causas de estas consultas.

2.1.3 TLD inexistentes populares

Hay una variedad de etiquetas populares que no se han delegado en la raíz y que no existen en el espacio de nombres del DNS público de Internet. Entre los más populares de estos TLD inexistentes, se encuentran .home, .lan, .corp y .local. Estos TLD son clasificados de forma individual dado que todos ellos aumentaron de volumen durante nuestro estudio.

2.1.4 Otros

Esta categoría abarca todas las consultas que no se pueden clasificar en ninguna de las otras categorías que se describen anteriormente.

3 Observaciones

Las cuatro instancias de IMRS en Francia recibieron 5400 millones de solicitudes del DNS por semana, en promedio, entre las semanas 6 y 11 (ver Figura 6). Las mismas instancias recibieron 6900 millones de solicitudes del DNS en la semana 12. Esto representa un aumento del 28% en el tráfico de esos cuatro nodos de IMRS.

[3] “Variar la longitud de los nombres de detección de secuestro del DNS”. https://src.chromium.org/viewvc/chrome?view=revision&revision=249013

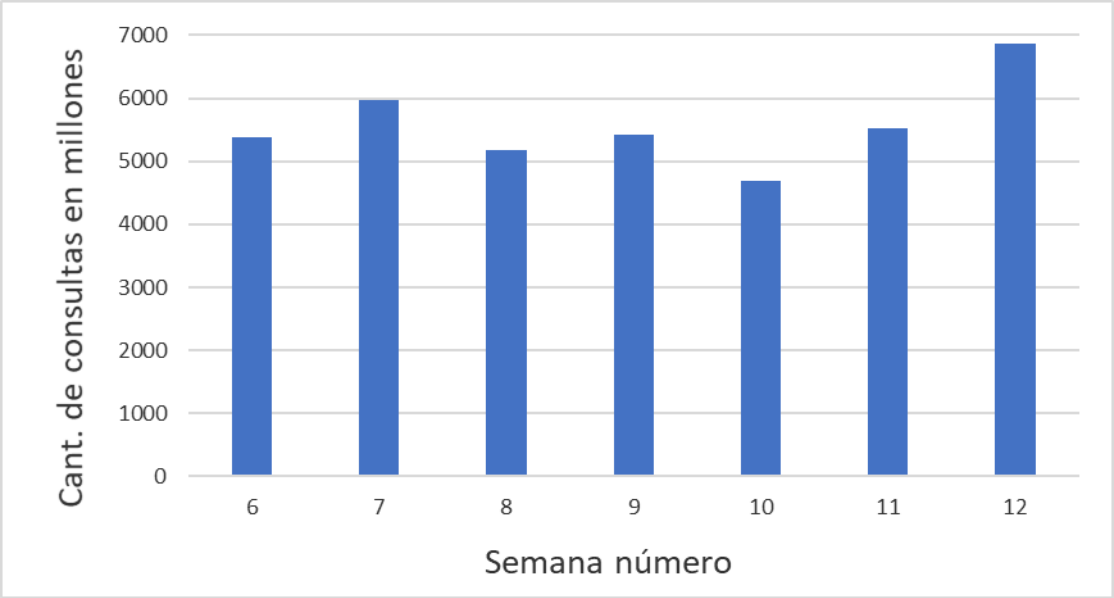

Figura 6: carga de consultas en las 4 instancias en Francia por semana desde la semana 6 hasta la semana 12.

Captamos algunas anomalías, como breves ráfagas de tráfico o instancias de interrupciones por mantenimiento en ese período de tiempo, pero tendían a ser de corta duración y no creemos que influyan significativamente en el tráfico total. Otros patrones de tráfico, como los patrones diurnos o fines de semana, también se absorben dado que el tráfico se acumuló durante una semana. No tenemos conocimiento de ningún otro cambio o evento en este período de tiempo que pueda influir en el volumen de consultas al DNS de manera tan significativa.

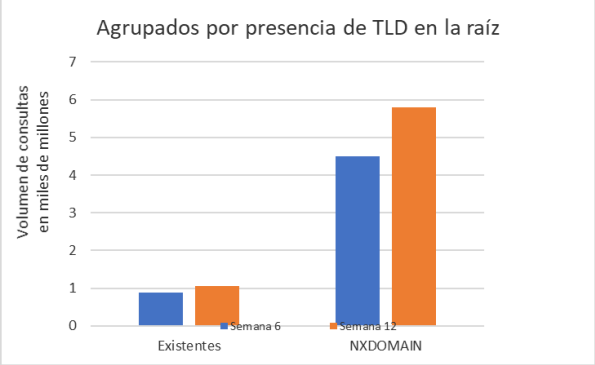

Figura 7: volumen de tráfico de TLD existentes e inexistentes en las semanas 6 y 12

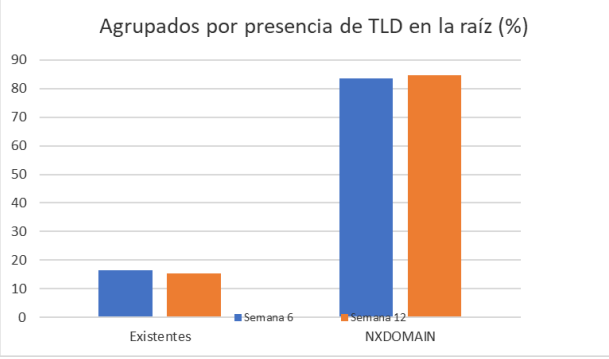

Figura 8: volumen de tráfico de TLD existentes e inexistentes en las semanas 6 y 12 como porcentaje del volumen total de esas semanas

En la figura 7, se muestra la diferencia en el volumen de consultas para los dominios existentes e inexistentes en números absolutos. Ambos grupos han crecido en volumen. La figura 8 muestra que también hay un pequeño cambio en la composición del tráfico, dado que el porcentaje de consultas de TLD existentes ha disminuido en comparación con las de los dominios inexistentes. El aumento del tráfico se debe principalmente a las consultas de dominios inexistentes.

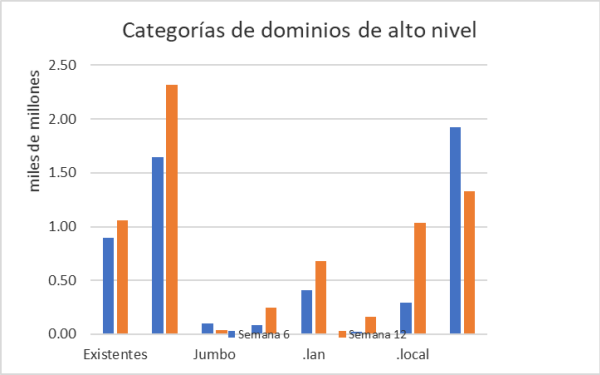

Figura 9: desglose del tráfico en varias categorías, comparando las semanas 6 y 12 en números absolutos.

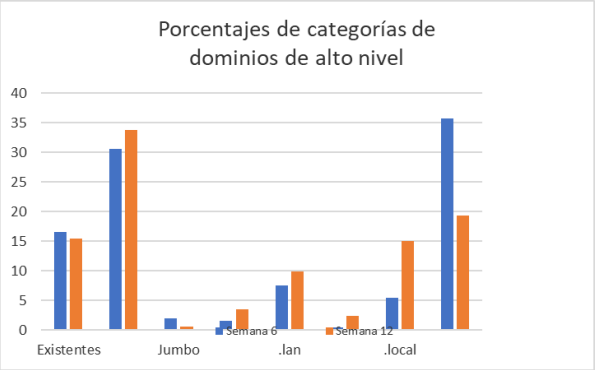

Figura 10: desglose del tráfico en varias categorías, comparando las semanas 6 y 12 como porcentaje del volumen total.

3.1 Consultas Chromium

Observamos que el 31 % de las solicitudes recibidas en la semana 6 y el 34 % en la semana 12 entran en la categoría de solicitudes del DNS de Chromium. Esto sigue siendo una parte significativa del tráfico total. Después del confinamiento, el número total de solicitudes aumentó un 28 %, mientras que la parte de Chromium de esas solicitudes aumentó un 41 %. El aumento se debe probablemente a que más dispositivos se conectan más a menudo debido a los mandatos de quedarse en casa.

Debido a las consultas de detección de redireccionamiento del DNS de Chromium, habrá un mayor índice de solicitudes del DNS para cadenas aleatorias de entre 7 y 15 caracteres de longitud visibles en el tráfico cuando se conecten más dispositivos con navegadores basados en Chromium. Cabe señalar que las consultas de solicitudes del DNS de Chromium no han aumentado en el mismo porcentaje que el tráfico total. Esto indica un ligero cambio en la composición del tráfico total. En otras categorías se ha registrado un aumento mayor que en las consultas de Chromium.

Las consultas de Chromium son la mayor causa individual de consultas a los servidores raíz. Otras instancias de IMRS a menudo registran más del 50 % de todas las consultas entrantes de Chromium. El propósito de estas consultas es comprobar si Chromium está detrás de un portal cautivo. El aprovisionamiento de los servidores raíz suele depender de la carga total de los servidores raíz para satisfacer las necesidades de ampliación. Si bien estas consultas son gratuitas para Chromium, el costo del aprovisionamiento de las instancias del servidor raíz no lo es. Google ha sido notificado de este problema, pero sigue pendiente.[4]

3.2 Consultas Jumbo

Hemos observado que ha disminuido el volumen de solicitudes con dominios de TLD largos (más de 15 caracteres). No hemos investigado la razón de este descenso del tráfico.

[4] Las tres sondas aleatorias del detector de redireccionamiento de la intranet no tienen un TLD y, por lo tanto, llegan a los servidores raíz.
https://bugs.chromium.org/p/chromium/issues/detail?id=946450&q=intranet%20redirect&can=2

3.3 TLD inexistentes populares

Los cuatro TLD inexistentes más populares que registraron un aumento en el volumen fueron .corp, .home, .lan y .local. De estos, .corp, .lan y .local registraron el aumento más significativo. Esto se debe probablemente a que la gente trabaja más desde su casa. Normalmente, los trabajadores se congregan en oficinas que utilizan un conjunto de resolutores que comprenden cómo responder a los dominios .corp, .lan y .local. Ahora, están más dispersos y trabajan desde la casa y utilizan resolutores que pueden no entender cómo responder a estos dominios. Esto también explicaría el aumento de las consultas en .home: más gente utiliza Internet más a menudo desde sus casas.

4 Conclusión

Los efectos de los confinamientos a nivel nacional para contener la pandemia global han tenido un efecto limitado, aunque notable, en el tráfico del DNS en las instancias de IMRS cuando se observaron a nivel de país. Este aumento del tráfico del DNS puede observarse en general. El hecho de que no se hayan registrado problemas sugiere que la arquitectura del DNS tiene la capacidad para ampliarse durante los escenarios de trabajo a distancia y el aumento del uso en el hogar.

Autores: Adiel Akplogan, Roy Arends, David Conrad, Alain Durand, Paul Hoffman, David Huberman, Matt Larson, Sion Lloyd, Terry Manderson, David Soltero, Samaneh Tajalizadehkhoob, Mauricio Vergara Ereche.