DNS open resolvers con IPv4 que involucran recursos bajo la administración de LACNIC

Autores: CSIRT CEDIA, LACNIC CSIRT
Coordinación/revisión: Graciela Martínez, Guillermo Pereyra

lacnic
www.lacnic.net

Índice

Resumen ejecutivo

El CSIRT de LACNIC y el CSIRT de CEDIA realizaron un estudio para identificar servidores de DNS abiertos asociados a una dirección IPv4, con el fin de informar a los asociados que tienen asignados estos recursos de la situación, sugerir alternativas para corregir la configuración de estos e intentar disminuir de forma significativa la cantidad de open resolvers en nuestra región. La comunicación se realizó por distintos medios para evaluar, además, la efectividad de cada uno.

Los *open resolvers* constituyen un riesgo de seguridad latente en la infraestructura de Internet, porque son servidores configurados de tal forma que permiten ser utilizados para atacar infraestructuras de terceros y llevar a cabo ataques de denegación de servicio.

Ya en marzo del 2013 US-CERT emitió su alerta TA13-088A,[1] en la que advierte del problema y propone medidas de mitigación.

[1] ‹https://us-cert.cisa.gov/ncas/alerts/TA13-088A›

Introducción

El principal vector de ataque para aprovechar vulnerabilidades en servicios sigue siendo a través de servicios expuestos por IPv4. Actualmente la mayoría de los ataques se ejecutan a través de servicios vulnerables que corren bajo este protocolo.

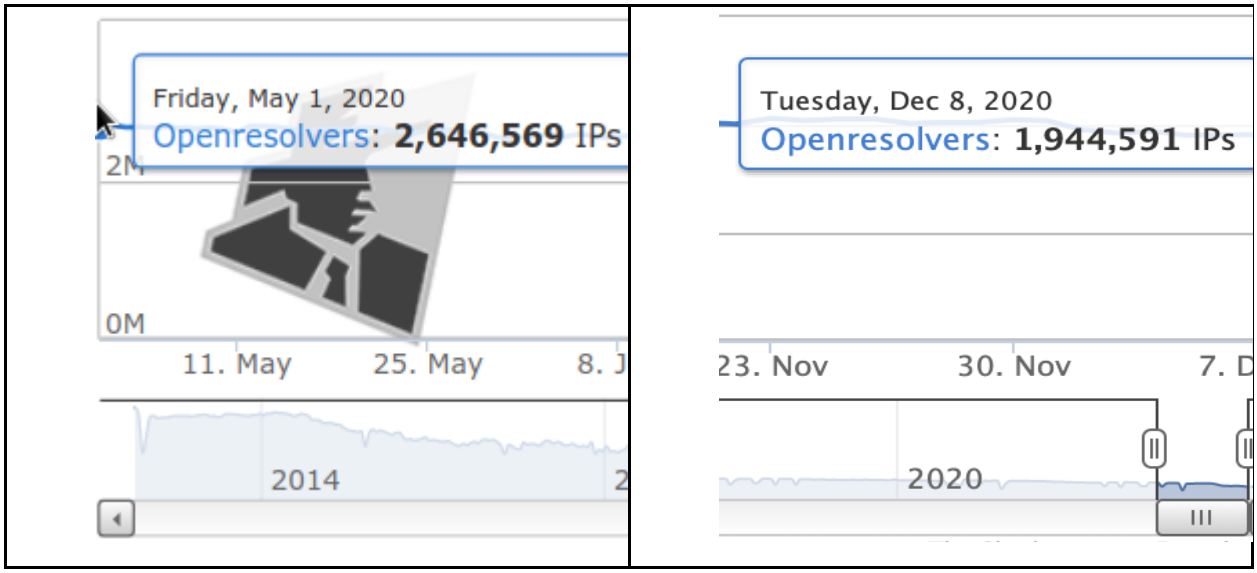
El uso del protocolo IPv4 representa una ventaja también para los CSIRT, por tratarse de un universo conocido, controlado y relativamente rápido de revisar para encontrar estas fallas. Existen herramientas muy eficientes que pueden encontrar en pocos minutos puertos abiertos en el universo de IPv4 (< 2^32 direcciones IP), más simple aun cuando el universo se reduce a los recursos asignados a un determinado RIR.

De acuerdo con el objetivo del proyecto, se buscó ubicar y reportar los servidores DNS que actúan como *open resolvers*. Un *open resolver* es aquel servidor de DNS que responde a las preguntas de resolución que se originan desde cualquier red, independientemente de que sea la red de un tercero o la suya propia.

Un *open resolver* es una amenaza para la seguridad y estabilidad de Internet, porque permite realizar actividades potencialmente dañinas. Estas se basan en la conocida técnica de amplificación del protocolo UDP. A través de esta, se busca que la respuesta a esta consulta haga llegar a la víctima escogida una gran cantidad de información. Para el caso de un *open resolver*, el atacante envía una pequeña consulta con una dirección origen falsa y con un tipo de *récord* que implique una respuesta muy grande (ej.: TXT, ANY o extensiones de DNSSEC).

Situación general

De acuerdo a datos de ShadowServer,[2] la cantidad mundial de *open resolvers* detectada en diciembre de 2020 disminuyó con respecto a la de mayo, pero de todas maneras la cifra de casi dos millones de servidores DNS que continúan abiertos es muy grande y representa una potencial amenaza a los diversos sistemas.



Impacto

Contar con servidores DNS abiertos impacta de diversas formas, no solamente a quien recibe el ataque, sino también a los proveedores y usuarios. Por ejemplo, en:

- **Reputación**: el responsable de la red que alberga el *open resolver* puede ver afectada su reputación al percibirse un descuido en los servicios que gestiona.
- **Calidad del tráfico**: el tráfico que se genera desde esta red es innecesario y podría evitarse, ya que seguramente afecte el tráfico legítimo y/o a los sistemas que manejan el tráfico de la red.

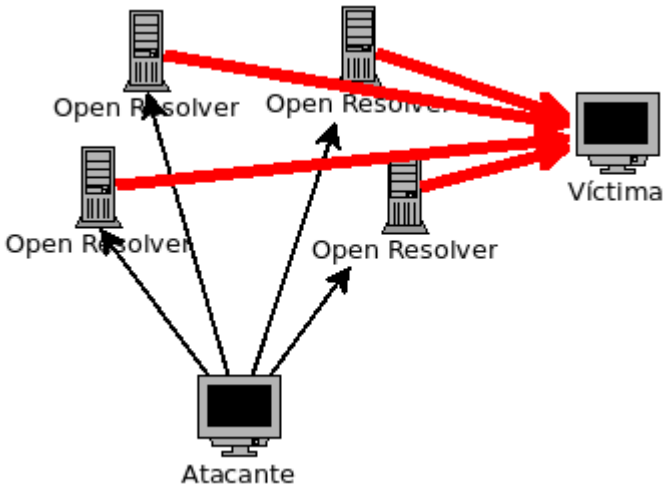
En muchos de estos casos, las organizaciones no conocen de la existencia de este problema de seguridad en su red y, por tanto, no actúan ni en la prevención ni en la resolución del problema.

La notificación de este problema ayuda a la institución a trabajar para corregirlo o, al menos, a tomar conocimiento de su existencia. En caso de no tener los recursos necesarios para su corrección, podrá justificar su contratación.

[2] ‹https://scan.shadowserver.org/dns/stats/›

Ataque de denegación de servicio por inundación de paquetes

A continuación, se ilustra el *modus operandi* de un ataque de denegación de servicio por inundación de paquetes. El atacante hace la misma consulta a diversos *open resolvers*, pero las realiza con la dirección de origen de la víctima. Sus consultas son de un tamaño muy pequeño y significan un consumo bajo de recursos para él, pero la víctima —que es quien recibe las respuestas de todos los *open resolvers*— sentirá el impacto de una enorme cantidad de información que le llega (y que no solicitó), que le ocasionará sin duda un agotamiento de sus recursos.



¿Qué mecanismos hay para detectar un *open resolver*?

El proceso de detección de un *open resolver* consiste en conocer si se obtiene una respuesta a una consulta realizada al puerto 53/UDP de una determinada IP. En caso afirmativo, es un *open resolver*.

Sin embargo, es muy costoso enviar una consulta a todas las IP del universo de redes, aun cuando solo se intente hacerla a los recursos IPv4 bajo la administración de LACNIC. Es por esta razón que se hace una consulta DNS recursiva solamente a las IP que tengan el puerto 53/UDP abierto.

Cabe destacar, además, que este proceso es solamente el resultado de una instantánea tomada al momento de realizar la consulta. Las respuestas pueden variar en gran medida entre cada encuesta realizada, porque dependen de factores como *timeouts*, equipos apagados, respuestas no esperadas, bloqueos por parte de IPS/*Firewalls*. Por esto, es importante monitorear continuamente los *open resolvers* para poder ir encontrando los que pueden no aparecer en búsquedas anteriores.

Herramientas y fuentes de datos relacionados con el tema

Como primer paso en la investigación, se evaluaron varias técnicas, herramientas y fuentes de datos referidos al tema.

Herramientas

Dig / Host

Permiten revisar si una determinada IP responde a un *query* al servicio de DNS. Para ello, es necesario indicar la IP que se revisará. No aceptan rangos, solo una IP a la que consultarán. Si la IP responde, se puede considerar que es un *open resolver*; si no responde, significa que no se tiene evidencia de que sea un *open resolver*.

Ambas funcionan apropiadamente para el objetivo del proyecto. Escogimos Dig para las validaciones.

NMAP

Herramienta muy conocida, que permite revisar un rango o red y encontrar puertos abiertos en esta red.

Masscanner

Variante similar a NMAP. De hecho, utiliza prácticamente los mismos *switches*. Se le puede proveer una lista de redes o IP y los puertos a encontrar abiertos y entregará un listado con los resultados de esta revisión.

Fuentes de datos

Shodan

Se consultó a través de Shodan para obtener listas de DNS abiertos en la región y se encontraron dos limitaciones:

- La lista no se actualiza diariamente. Se puede obtener un reporte de 53 puertos abiertos, que no significa que sean *open resolvers*.
- El listado que se obtiene se actualiza de forma inespecífica en el tiempo.

Shadowserver[3]

Se contactó a Shadowserver. Aunque se esperaba un conjunto muy similar de resultados, la realidad es que estos difieren de los obtenidos. En algunos casos se encontraron *open resolvers* que no estaban en la lista de Shadowserver; en otros casos, ocurrió a la inversa. Esta diferencia puede deberse a diversos aspectos. Por ejemplo: el RIR al que pertenece la red no es siempre LACNIC, la hora en que se hizo la revisión, bloqueos que pueden existir para impedir que se acceda de ciertas redes, tiempos de respuestas prolongados, etc.

Eventualmente, se pensó en consolidar o contrastar los datos de ambas fuentes, pero —al no ser conocido el universo de IP usado por Shadowserver— se podrían haber contaminado nuestros resultados, en lugar de enriquecerlos.

Delegated extended de LACNIC

Por lo expuesto se decidió utilizar la información recabada directamente del *delegated extended* de LACNIC.

---

[3] ‹https://www.shadowserver.org/›

Procedimiento seguido

A continuación, se describe el procedimiento utilizado para el escaneo.

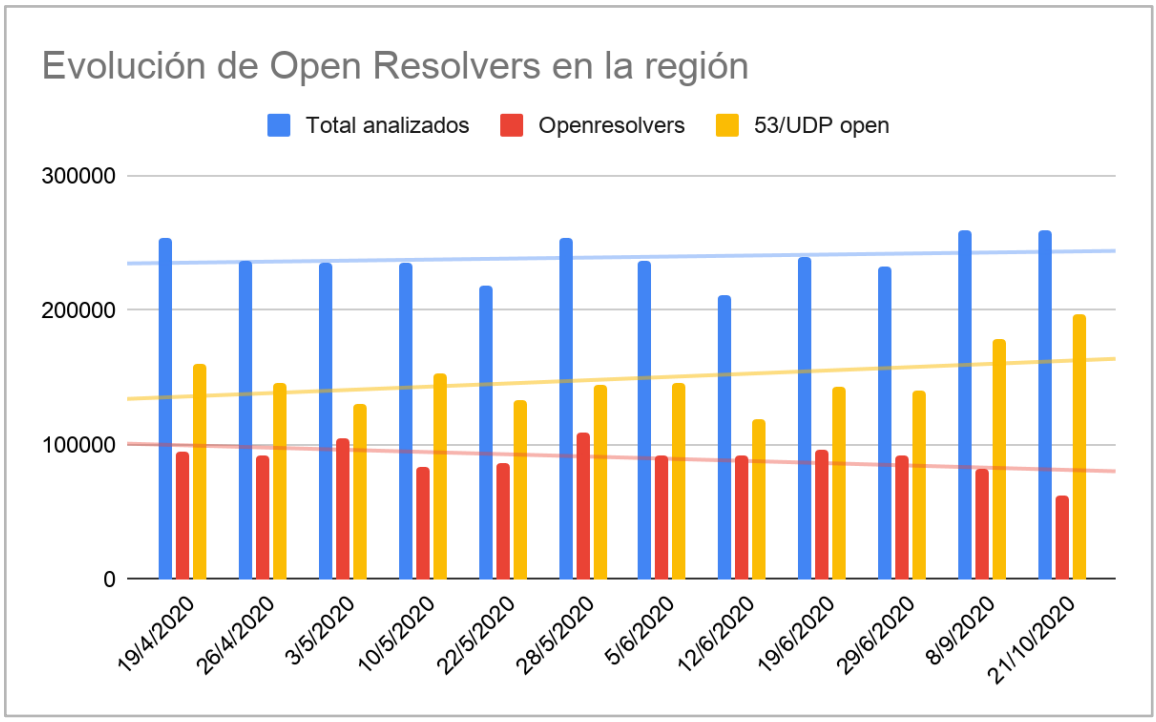
1. Se descargó la lista LACNIC-extended del ftp que contiene las subredes asignadas en la región que atiende LACNIC.
2. Se convirtió este resultado a CIDR.
3. Se realizó un *supernetting* a estos rangos y se alimentó al *masscanner* con esta lista.
4. Usando *masscanner* se buscaron puertos 53/udp abiertos en esta lista.
5. Del resultado de IP con este puerto abierto y utilizando el comando *dig*, se buscaron los servidores de dominio que responden a una consulta específica y propia de un dominio bajo control de CEDIA: test-csirt.cedia.org.ec (TXT).
6. Se obtuvo la lista de contactos de los positivos del paso anterior.
7. Se separaron los recursos bajo la administración de los NIR.
8. Se organizaron y se enviaron estos avisos por tres vías diferentes (correo electrónico, contacto directo con el responsable del rango y a través del módulo de seguridad de MiLACNIC).
9. Los avisos contenían además sugerencias de solución (ver anexo 1). El procedimiento descrito se depuró y ejecutó en tres ocasiones.

Para comparar, siempre se mantuvieron como universo de estudio las primeras IP que fueron clasificadas como *open resolvers*.

Cantidad de *open resolvers* detectados durante el análisis

Del total de IP analizadas, se confirmaron como *open resolvers* solo aquellas que poseían el puerto 53/UDP abierto y respondieron preguntas de resolución DNS. Aquellas IP que no respondieron a las consultas fueron registradas solamente como puerto 53/UDP open.

En la gráfica que está a continuación, se muestra la evolución de la cantidad de servidores *open resolvers* abiertos al mundo durante el período del proyecto. Se puede observar que hubo una disminución.



Análisis y evaluación de acciones para informar sobre los DNS abiertos

Los contactos se realizaron utilizando tres canales: correo electrónico, contacto directo y MiLACNIC.

Del conjunto de IP asociadas a un servicio de DNS abierto al mundo, por un lado, se separaron los que están bajo la administración de los NIR, NIC.Mx y NIC.Br y con resto de la lista se armaron tres subconjuntos. A cada uno se le asignó un canal de los siguientes:

1. **Correo electrónico:** se envió un correo electrónico a los contactos registrados para cada IP de Argentina, Chile y Colombia.
2. **Contacto directo:** se contactó por diversas vías a los responsables conocidos de las cinco organizaciones con más *open resolvers* encontrados. Estos pueden o no haber sido los contactos registrados para cada IP. Se usaron técnicas sociales (llamar a personas conocidas en la organización).
3. **MiLACNIC:** se envió el aviso a través del portal de MiLACNIC (quedaron excluidos Brasil, México, Argentina, Chile y Colombia, por estar en alguno de los anteriores canales)

Resultados asociados a los canales de comunicación

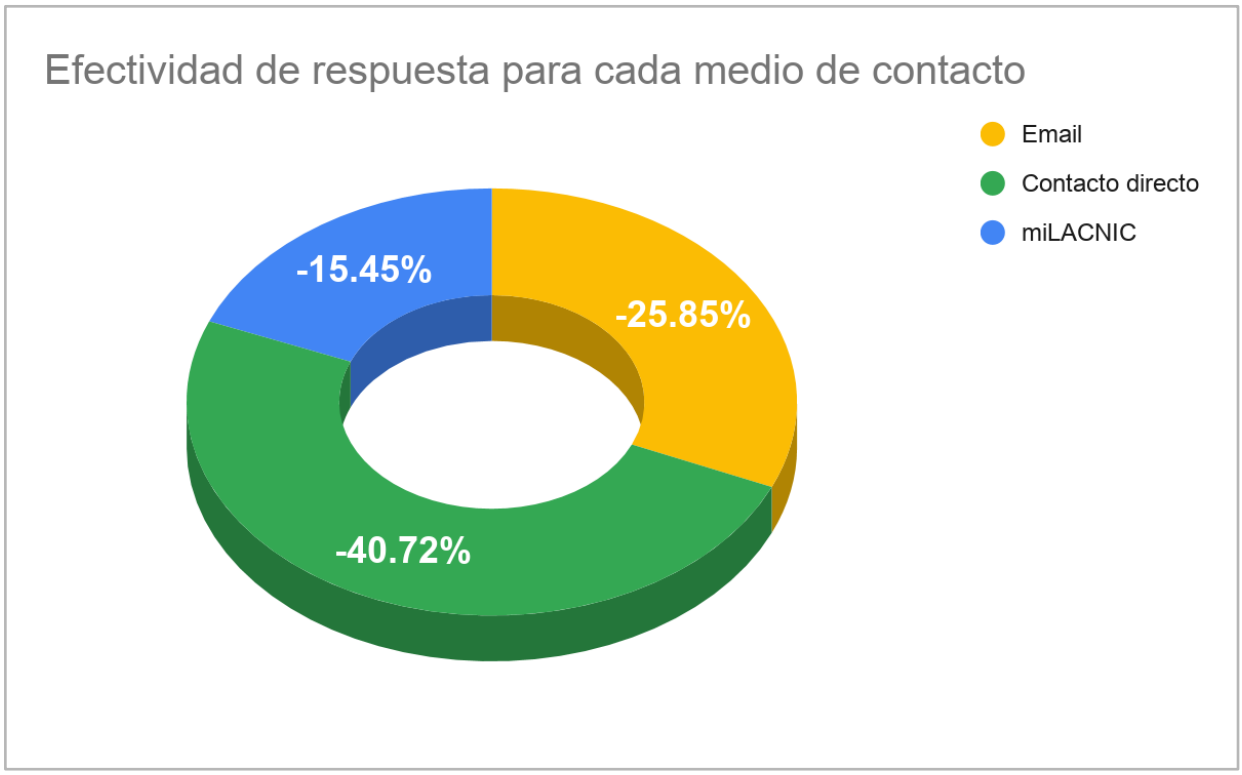
En la tabla que sigue se muestra la cantidad de recursos identificados como *open resolvers* en cada una de las rondas realizadas y el canal de comunicación utilizado.

Canal de comunicación utilizado	2020-06-29 1.ª ronda	2020-09-08 2.ª ronda	2020-10-21 Última ronda	Diferencia (%) 1.ª vs. última
Correo electrónico	19084	10920	14151	-25.85
Contacto directo	5545	3191	3287	-40.72
MiLACNIC	11436	7317	9669	-15.45
Total	36065	21428	27107	-24.84

Es de interés compartir algunos comentarios relacionados con estos resultados.

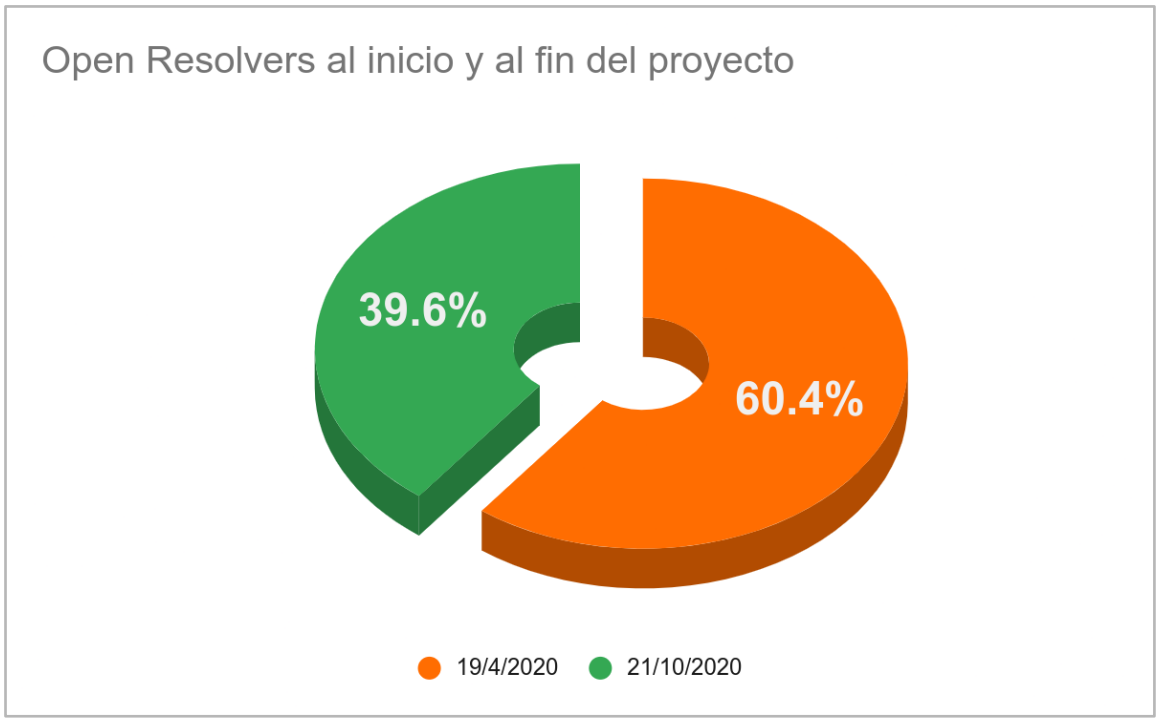
- Por correo electrónico se recibieron respuestas como:
  - Agradecimiento por el aviso y comunicación de que se tomarían acciones correctivas.
  - Notificación de que se habían realizado las acciones sugeridas y de que el problema estaba solucionado.
  - Solicitud de ayuda adicional.
- Más del 12% de los mensajes enviados por correo electrónico en la primera ronda rebotaron, porque la casilla de contacto que figura en el *whois* no es correcta.
- Si bien por contacto directo durante la primera ronda solo se recibió una respuesta a la notificación, los resultados muestran que se llevaron a cabo acciones, pues se vio una drástica disminución de los *open resolvers* abiertos.
- A través de MiLACNIC, no se recibió *feedback* de las organizaciones.

En gráfica que sigue se puede comparar el porcentaje de éxito según el canal de comunicación usado. Se considera *éxito* que el servidor responda a la consulta realizada.



Conclusiones

En líneas generales, podemos considerar que el resultado fue exitoso, ya que se logró disminuir un gran número de servidores DNS abiertos a consultas, como lo muestra el siguiente gráfico.



Se identificó al correo electrónico como el canal más efectivo para advertir a la comunidad objetivo sobre las vulnerabilidades de seguridad de sus sistemas y para ayudar a su corrección.

En esta misma línea, se concluye que existen muchas casillas técnicas o de *abuso* a las que no se pueden enviar reportes por diferentes razones. Es necesario que las organizaciones mantengan estas casillas funcionales y actualizadas para que se les pueda reportar sobre los incidentes de seguridad que pueden surgir.

Para lograr una reducción de los *open resolvers* en la región, es necesario automatizar el procedimiento de detección y aviso a los responsables. El reporte a las organizaciones sería una combinación entre envío de correo electrónico y el uso del módulo de seguridad de MiLACNIC.