Estudio de recursos de Internet presentes en la región de LACNIC con protocolos UDP que posibilitan ataques de tipo DDoS

(Ref. Estudio SSR 2021)
Informe final

Autores: Paula Venosa, Nicolas Macia, Guillermo Pereyra
Coordinación/revisión: Graciela Martínez
Edición: Carolina Badano, María Gayo, Martín Mañana
Proyecto: Fortalecimiento de Infraestructura de Internet Regional
Área: CSIRT LACNIC

lacnic
www.lacnic.net

Resumen ejecutivo 3
Abstract 3
Objetivo 3
Motivación 3
Análisis preliminar del problema 5
Introducción 5
Posibles protocolos amplificables 5
Fuentes de información 6
Análisis de protocolos de interés para el estudio 7
Relevamiento inicial 11
Fuentes de información utilizadas en el relevamiento 11
Resultados preliminares 12
Análisis 15
Acciones realizadas 16
Resultado de las acciones 19
Conclusiones 25
Referencias 26

Resumen ejecutivo

Este estudio logró identificar y mitigar vulnerabilidades sobre protocolos utilizados en la región para realizar ataques de denegación de servicios, con lo que logró una mejora en el nivel de seguridad de Internet.

Asimismo, propició la interacción entre el CSIRT de LACNIC y sus asociados en temas de seguridad, fortaleciendo el rol del equipo para compartir herramientas que permitan a las organizaciones que integran LACNIC dar un mejor servicio.

La investigación identificó vectores que se usan en los ataques y, entre ellos, una lista de protocolos sobre UDP que pueden amplificar el tamaño de su respuesta. También posibilitó al CSIRT de LACNIC trabajar directamente con organizaciones afectadas y reducir sus riesgos.

Abstract

Este informe refleja el trabajo realizado para relevar el problema relacionado con la presencia de servicios del User Datagram Protocol (UDP) amplificables, que pueden ser utilizados para ataques de DDoS (denegación de servicio distribuido) en América Latina y el Caribe.

El trabajo describe la metodología aplicada, los resultados obtenidos de un relevamiento inicial, las primeras recomendaciones para la mitigación y un análisis de situación posterior, en función de esas acciones.

Objetivo

Mejorar los niveles de ciberseguridad de los recursos IP bajo la administración de LACNIC, ayudando a la estabilidad y resiliencia de Internet, minimizando el posible uso de los protocolos UDP en ataques DDoS.

Motivación

Los ataques DDoS de amplificación son de los más frecuentes que sufren las organizaciones hoy en día. Aprovechan dos fallas en los protocolos de red:

- La información del encabezado IP no está autenticada.
- UDP no emplea un *handshaking*.

Estos ataques tienen gran impacto en la comunidad, porque presentan grandes ventajas a los atacantes. En primer lugar, al usar servicios vulnerables como reflectores de tráfico, ocultan inherentemente la dirección del atacante, lo que dificulta la detección del origen del ataque y las posibles acciones de mitigación.

En segundo lugar, pequeñas solicitudes a distintos reflectores suelen ser suficientes para desencadenar grandes respuestas. Esto puede ser utilizado para generar y dirigir grandes volúmenes de tráfico hacia una organización víctima objetivo. Dependiendo del protocolo del que un ataque de DDoS se está aprovechando, se pueden lograr factores de amplificación de 100x o más [1][2].

Este estudio enfatiza la necesidad de generar conciencia para minimizar la cantidad de dispositivos conectados a Internet que, por desconocimiento de quienes los administran, puedan ser usados para montar ataques de DDoS.

Análisis preliminar del problema

Introducción

Un ataque de denegación de servicio distribuido —llamado también DDoS— es generado, desde distintos orígenes, para causar que un servicio, recurso de Internet o red quede inaccesible. Los ataques de DDoS pueden afectar los recursos de una organización víctima durante el tiempo que el ejecutante desee. Dependiendo del volumen de tráfico recibido, puede afectar no solo a la organización víctima, sino también a su proveedor de Internet.

Una forma de llevar a cabo estos ataques es aprovechar la presencia de servicios reflexivos y amplificables expuestos a Internet. Los servicios reflexivos son aquellos que no necesitan de un *handshake* previo para el intercambio de datos. De esto se desprende que cualquier servicio que utiliza UDP como transporte podría entrar en esta categoría.

El otro requisito es que el servicio, además de ser reflexivo, sea amplificable. Los servicios amplificables son aquellos que, ante un requerimiento determinado, dan una respuesta cuyo tamaño es mucho mayor que el del requerimiento. A esta diferencia se la conoce como *factor de amplificación*.

Posibles protocolos amplificables

Distintos protocolos de Internet entran en la categoría de reflexivos y amplificables. Algunos, como CHARGEN, no deberían estar expuestos a Internet. Otros, como NTP, pueden presentar vulnerabilidades en el servidor que lo implementa.

Por último, cabe mencionar que malas configuraciones, por ejemplo en NTP o DNS, pueden permitir exponer servicios reflexivos con amplificaciones indeseables.

La alerta TA14-017A del Sistema Nacional de Concienciación Cibernética del US-CERT [3] identifica distintos protocolos basados en UDP que podrían ser potencialmente utilizados en

ataques de DDoS. En esta alerta se informan estos protocolos, su factor de amplificación y el comando vulnerable asociado.

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—
WS-Discovery	10 to 500	—

La alerta, originalmente publicada en el año 2014, se fue actualizando y se fueron incorporando nuevos protocolos vulnerables que podrían ser explotados o que fueron utilizados en ataques de DDoS que generaron grandes volúmenes de tráfico [4][5][6][7][8].

Adicionalmente, en una alerta del FBI del 2020 y en diversos sitios dedicados al análisis de problemáticas de DDoS a partir del resultado de ataques realizados, se mencionan protocolos que complementan los observados antes por la alerta TA14-017A. Entre ellos cabe mencionar CoAP, un protocolo de transferencia web diseñado para redes y dispositivos con recursos limitados, con potencial para desarrollar aplicaciones en *Internet of things* (IoT) [9][10][11].

En el futuro, esta lista de protocolos reflexivos y amplificables puede cambiar. Esto, por la posible aparición de nuevos protocolos vulnerables o el descubrimiento de nuevas formas de utilizar protocolos existentes para provocar amplificaciones hasta el momento inesperadas.

Fuentes de información

Existen distintas maneras de detectar dispositivos que exponen protocolos reflexivos y amplificables a Internet. La mejor forma de determinar la existencia de un protocolo

vulnerable es conectarse a cada posible recurso IP e intentar realizar una consulta inocua usando ese protocolo. En este sentido, vale la pena mencionar el proyecto SCANNING de la fundación Shadowserver, el cual, entre otras cosas, intenta identificar la presencia de recursos en Internet implementando protocolos amplificables y reflexivos[12][13].

Alternativamente, se pueden utilizar otras fuentes de información abiertas que brinden inteligencia de amenazas u OSINT. Como ejemplos de este tipo de fuentes de información abierta podemos mencionar SHODAN o CENSYS, que pueden ser utilizados para encontrar servicios amplificables vulnerables[14][15].

Sin embargo, que un protocolo esté expuesto no significa necesariamente que sea vulnerable y pueda ser explotado. Por ejemplo, un servidor de DNS es vulnerable si está configurado como *open resolver* sin ningún tipo de restricción en su uso. Debido a esto, dependiendo el protocolo evaluado, puede ser necesaria una posterior verificación de la vulnerabilidad del servicio.

Análisis de protocolos de interés para el estudio

Si bien lo ideal es erradicar todos los protocolos vulnerables a ataques de amplificación, se seleccionaron aquellos que pueden representar mayor riesgo para la seguridad y estabilidad de Internet. Para la selección, se tuvieron en cuenta:

- Los protocolos reflexivos y amplificables que se conoce que son utilizados en estas problemáticas.
- Nuevos protocolos vulnerables observados en los últimos años.
- El factor de amplificación posible que cada protocolo puede ofrecer a un atacante.
- La cantidad de potenciales dispositivos vulnerables en Internet.
- Las fuentes de información con las que se puede contar.

Como punto de partida, tomamos los servicios que en principio pueden considerarse los exponentes más claros de esta problemática. Con ellos se utilizó Shodan, para tener una estimación rápida de la cantidad de dispositivos que exponen este servicio a Internet. Combinando esta información con el factor de amplificación de cada uno, se generó la siguiente tabla:

Protocolo	Factor de amplificación	Cantidad de dispositivos que exponen este servicio	Daño posible Cantidad * Factor de amplificación
NTP	4670.00	7088780	33104602600.00
Memcached	51000.00	553292	28217892000.00
DNS	98.30	8940561	878857146.30
WS-Discovery	500.00	190283	95141500.00
CharGEN	358.80	85667	30737319.60
SSDP	75.90	387702	29426581.80
CoAP	34.00	540208	18367072.00
SNMP	11.30	1534758	17342765.40
QOTD	140.30	61676	8653142.80

Algunas observaciones a partir de estos resultados son:

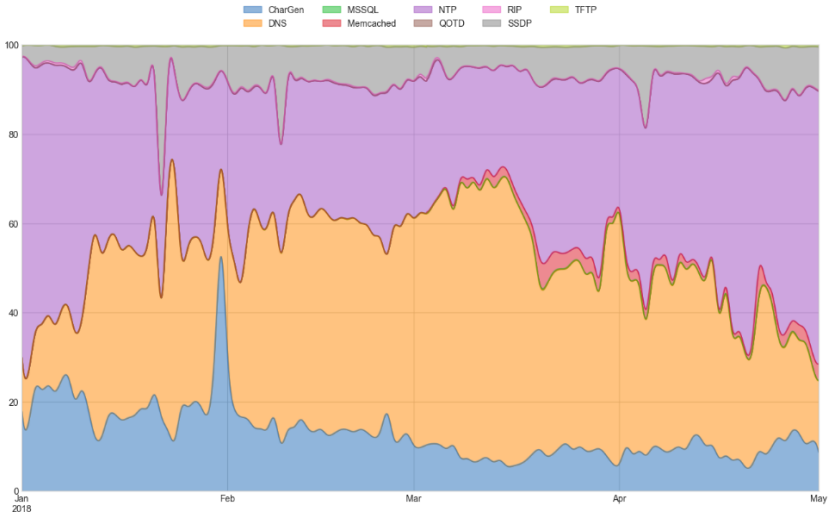
● No todos los dispositivos estimados por Shodan son reflexivos. Los siguientes protocolos pueden funcionar tanto sobre UDP como sobre TCP: Memcached, DNS, WS-Discovery, CharGen, SNMP y QOTD.

● Debido a que con Shodan no podemos consultar sobre los que corren exclusivamente sobre UDP, en principio no tenemos certeza de cuántos de estos se pueden utilizar para montar ataques de DDoS, lo cual es de interés para este estudio.

● Los protocolos informados por Shodan no distinguen versiones. Esto, en el caso particular de SNMP es de interés, puesto que la versión vulnerable es la 2c, la cual permite utilizar de manera reflexiva el comando GetBulk para lograr factores de amplificación elevados.

Adicionalmente, para la evaluación, se utilizó información de distintas fuentes, de modo de contrastar el riesgo que cada uno de estos protocolos representa hoy en día. En este sentido, si bien todos los problemas son graves, vale la pena mencionar que:

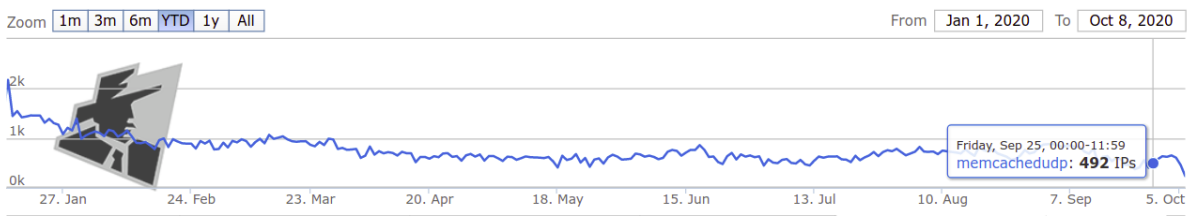
● Durante 2018, un estudio realizado por un proyecto financiado por la Unión Europea[https://sissden.eu/blog/amp2018] mostraba en los resultados de una red de *honeypots* que los ataques de DDoS observados evidenciaban la vigencia y relevancia del uso por parte de los atacantes de protocolos como CharGen, DNS, NTP y SSDP.



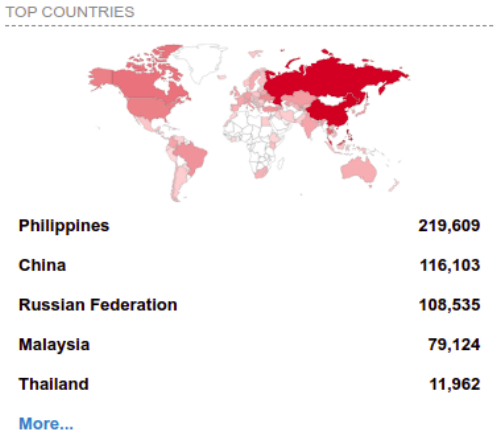
- Se analizaron los datos públicos de la fundación Shadowserver. La fundación Shadowserver reúne y analiza datos sobre actividades maliciosas de Internet. En particular, se utilizaron estadísticas públicas globales y por países sobre distintos protocolos que se pueden utilizar en ataques de DDoS.

- El protocolo Memcached irrumpió en la escena de los servicios reflexivos y amplificables en febrero de 2018, cuando fue utilizado para realizar, hasta ese entonces, el mayor ataque volumétrico de DDoS con el que Akamai experimentó 1.3. TBps sobre uno de sus clientes [8]. Desde ese momento se visibilizó el problema y se concientizó adecuadamente a la comunidad. Como resultado de esto, podemos ver estadísticas realizadas por la fundación Shadowserver que muestran la cantidad de servidores Memcached sobre UDP observados en Internet.

La gráfica empieza cuando sucedió el ataque de DDoS descripto. A partir de ahí, el descenso es visible. Los datos disponibles del 2020, los últimos publicados por Shadowserver, muestran mejor la escala sobre la cantidad de servidores reflexivos de este protocolo:



Respecto a CoAP, protocolo que se espera encontrar en distintos dispositivos de *Internet de las cosas* (IoT), existe un proyecto de la Unión Europa llamado VARIoT que intenta clasificar dispositivos vulnerables expuestos a Internet. De los resultados informados en el proyecto, la gran mayoría de los dispositivos vulnerables se encuentran en Filipinas, Rusia y China[10]. Esta información también fue contrastada con Shodan, el cual mostró que en la región de LACNIC no hay una cantidad significativa de dispositivos que implementen CoAP.



Por último, como parte de la evaluación de los protocolos de interés, se tuvo en cuenta la manera de definir si el servicio expuesto es vulnerable. En este sentido, se estudió, para cada uno de los protocolos analizados, si alcanza con hacer un requerimiento válido para determinar, en función de la respuesta, si el servicio es vulnerable.

Para WS-Discovery es necesario enviar un comando mal formado para constatar la vulnerabilidad del servicio expuesto. Mientras, para el resto de los protocolos se dispone de comandos válidos que permiten confirmar la vulnerabilidad del servicio sin poner en riesgo su normal funcionamiento. No consideramos adecuado incluir el protocolo WS-Discovery en el estudio, pues no se puede asegurar la inocuidad de los tests realizados contra dispositivos de este tipo.

En virtud de esos resultados, se define que es pertinente analizar y evaluar la problemática en la región, haciendo foco en la detección, concientización y mitigación de instancias vulnerables de servicios de los protocolos: NTP, DNS, CharGen y SSDP.

Relevamiento inicial

Como se entendió en la fase preliminar del estudio, es pertinente analizar y evaluar la problemática en la región, haciendo foco en la detección, concientización y mitigación de instancias de servicios vulnerables de los protocolos: NTP, DNS, CharGen y SSDP.

En la evaluación se relevaron distintas fuentes de información. Una vez logrados los resultados, se hizo un análisis y en función de ello se definieron las acciones de mitigación.

Fuentes de información utilizadas en el relevamiento

Para el estudio, además de la realización de pruebas propias, se utilizó la información provista tanto por Shadowserver como por Shodan. Se utilizó como fuente primaria Shadowserver, porque proviene del proyecto SCANNING,[1] que identifica, entre otros problemas, la presencia de recursos en Internet implementando protocolos amplificables y reflexivos tratados en este estudio.

Una ventaja significativa en el uso de Shadowserver como fuente de información es que el proyecto no se limita simplemente a realizar el escaneo de los servicios, sino que evalúa si estos son vulnerables al permitir ser utilizados en ataques de amplificación.

En el caso del protocolo CharGen, en el que la sola exposición del servicio es suficiente para considerarlo vulnerable, se utilizó Shodan como fuente primaria, puesto que se estableció contacto con Shodan y fuimos informados sobre la posibilidad de buscar instancias de dicho servicio corriendo sobre UDP. Para ello se realizó la búsqueda de la siguiente manera: *«port:19 shodan.module:newline-udp».*

La experiencia resultó por demás interesante, puesto que las instancias TCP de dicho servicio no son vulnerables por no ser TCP un protocolo reflexivo (como sí es UDP).

---

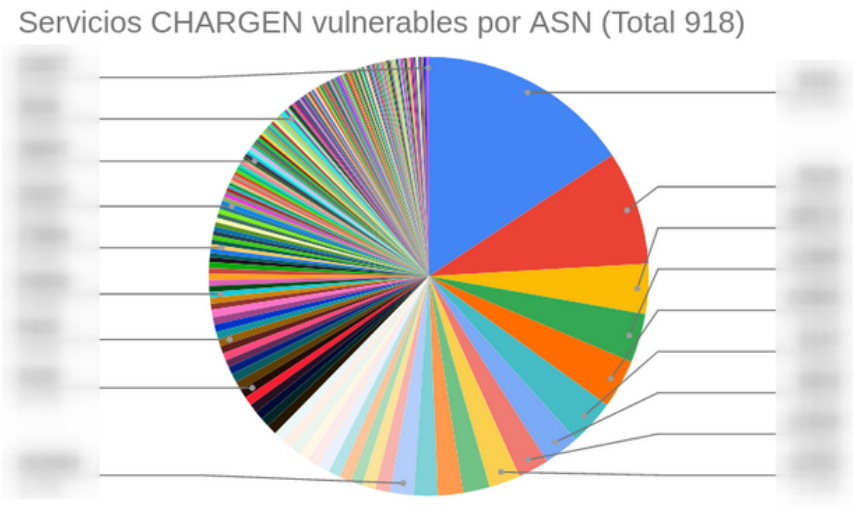
[1] https://scan.shadowserver.org/

Adicionalmente, se realizaron pruebas manuales para corroborar la información provista por las fuentes de información utilizadas. También, para analizar posibles situaciones que despiertan interrogantes, como la observada respecto del servicio SSDP informado por Shadowserver, que detecta la presencia de dicho protocolo en diferentes puertos UDP.

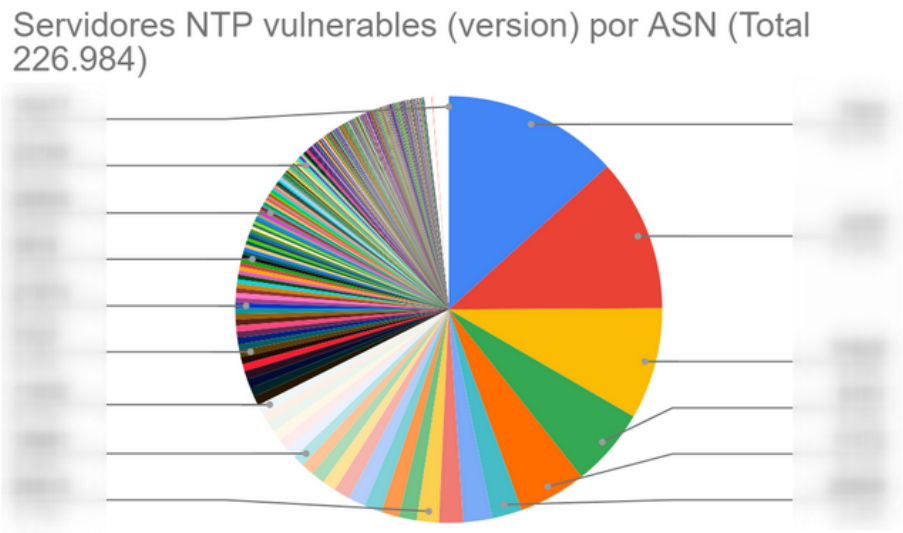
Resultados preliminares

De los reportes obtenidos se definieron distintas vistas para presentar la información de las problemáticas, utilizando diferentes sumarizaciones: problemas por sistema autónomo, problemas por país. Dado que la sumarización por país no refleja cuestiones propias de cada uno, sino que simplemente va de la mano del tamaño de estos, se prefirió hacer el análisis de cada una de las problemáticas previstas en los protocolos analizados por sistema autónomo.

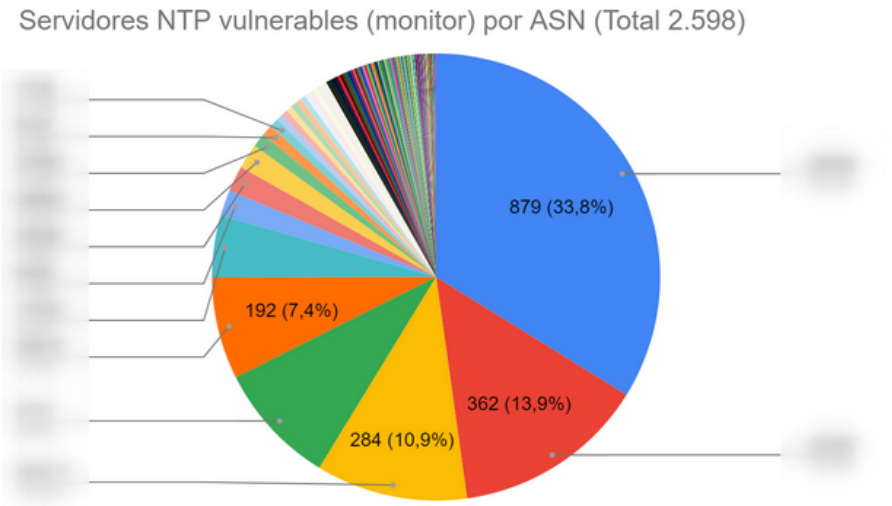
En el siguiente gráfico se muestran los porcentajes de servicios CharGen vulnerables por ASN. El total de servicios vulnerables hallados para toda la región fue de 918.



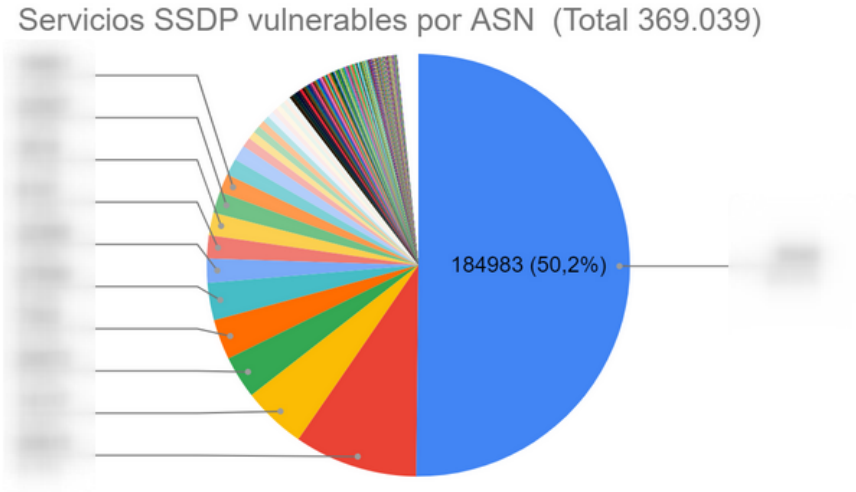
En el siguiente gráfico se muestran los porcentajes de servidores NTP por ASN que admiten consultas tipo READVAR (Mode 6). El total de servidores vulnerables hallados para toda la región fue de 226.984.



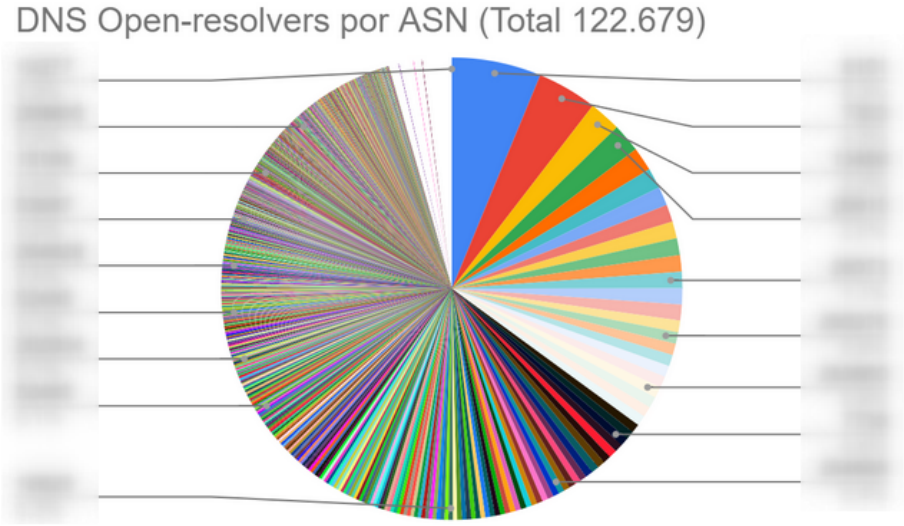
En el siguiente gráfico se muestran los porcentajes de servidores NTP por ASN que admiten consultas tipo MONLIST (Mode 7). El total de servidores vulnerables hallados para toda la región fue de 2598.



En el siguiente gráfico se muestran los porcentajes de servicios SSDP vulnerables por ASN. El total de servicios vulnerables hallados para toda la región fue de 369.039.



En el siguiente gráfico se muestran los porcentajes de DNS *open resolvers* por ASN. El total de DNS *open resolvers* hallados para toda la región fue de 122.679.



Análisis

El procesamiento de la información de manera gráfica permitió pensar una estrategia para el reporte de las problemáticas, maximizando las vulnerabilidades que se gestionarán. Por eso, a partir de estos, se realizaron las siguientes observaciones y determinaciones:

● En base a los datos obtenidos sobre los protocolos **NTPversion** y **NTPmonitor** se decidió realizar reportes por separado de estas problemáticas, de manera de gestionar adecuadamente los problemas de cada tipo.

● Se observó que en el caso del protocolo SSDP existe una disparidad muy grande entre el sistema autónomo que más problemas presenta, respecto al resto. Esto incluso provoca que el país al que pertenece dicha organización figure en el Top 20 de las estadísticas de Shadowserver por los problemas en este ASN.[2]

● Aprovechando que un gran porcentaje de vulnerabilidades detectadas para los protocolos CharGen, SSDP y NTP se concentraba en unas pocas organizaciones, se propuso realizar el reporte a aquellas tres con más problemas hallados (por protocolo) considerando:

- Maximizar el porcentaje de vulnerabilidades a gestionar.
- Incluir organizaciones de distintos países para abarcar e incluir en posteriores fases de concienciación diferentes regiones geográficas del área de cobertura de LACNIC.

● Para el caso de DNS *open resolvers*, dada la uniformidad observada en la cantidad de ocurrencias detectadas por organización, se propuso realizar el reporte a las cinco organizaciones con más instancias de DNS *open resolvers*, considerando incluir, al igual que en el caso anterior, organizaciones de distintos países.

● Respecto al protocolo SSDP, cabe mencionar que los reportes de Shadowserver mostraron la inclusión de dispositivos corriendo en otros puertos, de los cuales el puerto 1900 no fue el más utilizado.

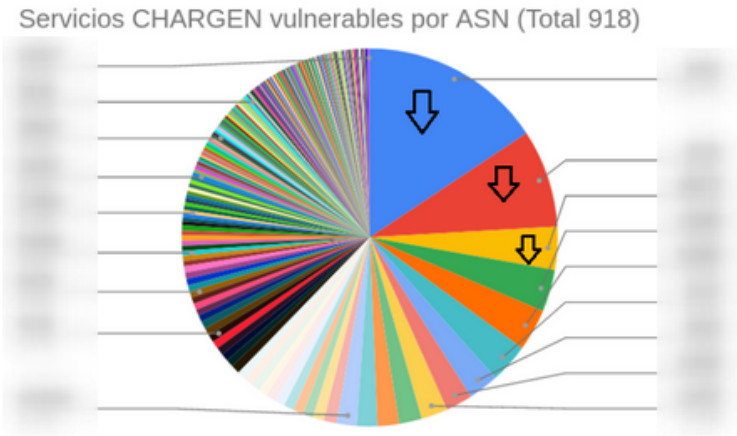
[2] https://scan.shadowserver.org/ssdp/

Acciones realizadas

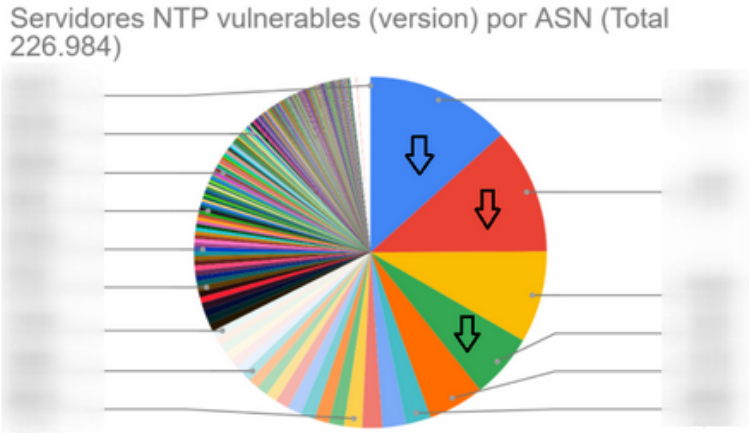
El trabajo de investigación realizó las siguientes acciones:

● Seleccionó a las organizaciones para reportar las vulnerabilidades de los distintos protocolos:

CharGen

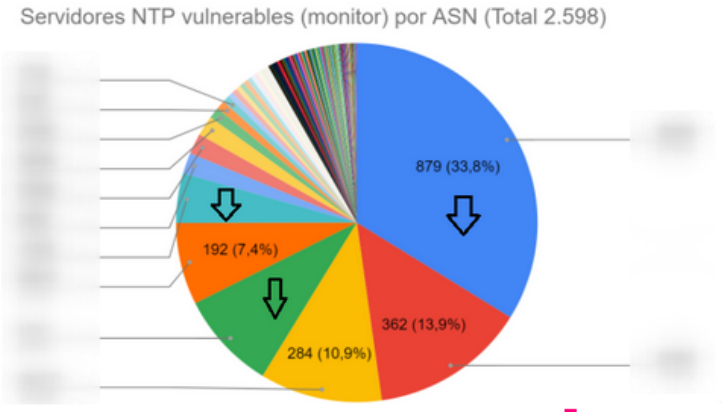


NTP (versión)



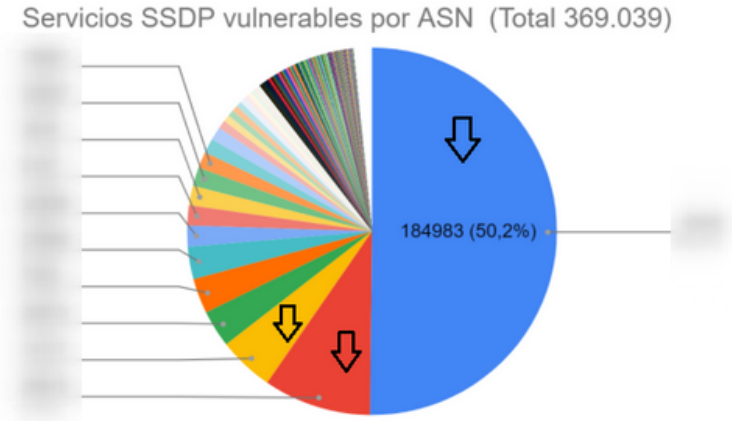
Nota: no se incluyó el tercer ASN para incluir organizaciones de tres países distintos y lograr mayor cobertura del proyecto en lo que refiere a la mitigación de esta vulnerabilidad.

NTP (monitor)

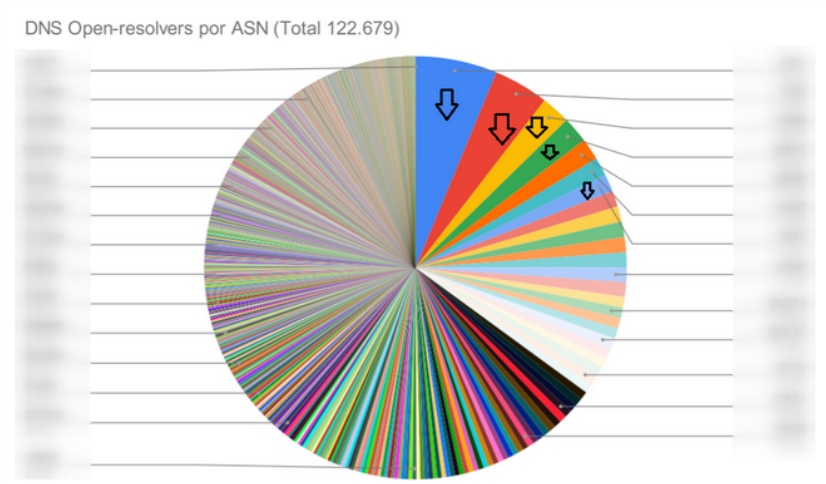


Nota: no se incluyeron el segundo, tercer y quinto ASN para incluir organizaciones de tres países distintos y lograr mayor cobertura de países en el proyecto, en lo que refiere a la mitigación de esta vulnerabilidad.

SSDP



DNS



Nota: no se incluyeron el quinto y sexto ASN para incluir organizaciones de cinco países distintos y lograr mayor cobertura de países en el proyecto, en lo que refiere a la mitigación de esta vulnerabilidad.

● Se buscaron puntos de contactos válidos para las organizaciones elegidas. En conjunto con LACNIC se buscaron los contactos asociados a partir de la información brindada por los servicios de WHOIS y RDAP. También se tuvo en cuenta la información de los CSIRT de nuestra comunidad para contar con un contacto alternativo en caso de ser necesario.

● Se contactaron doce organizaciones de países de la región. Una de ellas presentaba cuatro de las dificultades detectadas y otras dos de las problemáticas involucradas en este estudio.

● Se informó sobre los distintos tipos de hallazgos.

● Se generó la evidencia para presentar la problemática a los afectados de manera tal que estos puedan dimensionar el impacto.

● Se contactó a los asociados de LACNIC seleccionados que tienen servicios vulnerables. En un primer mensaje se explicó el objetivo del proyecto y se solicitó confirmación para saber si el contacto era pertinente, ofreciendo a partir de ello compartir la información específica de las vulnerabilidades halladas.

En función de las necesidades de las organizaciones contactadas con el objeto de dar soporte:

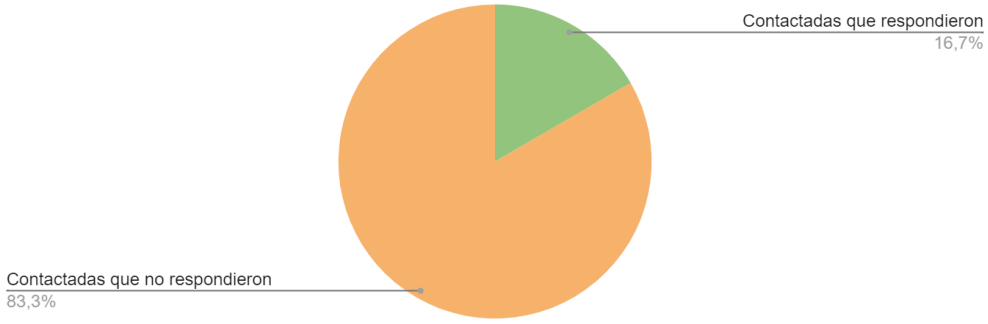
● Se programaron reuniones para trabajar en conjunto con los asociados afectados de manera tal de mitigar las vulnerabilidades halladas, mejorando así el nivel de seguridad de la región.

● Se respondieron consultas e inquietudes por correo electrónico, tanto para dar soporte en la mitigación como para verificar la correcta solución de las problemáticas informadas.

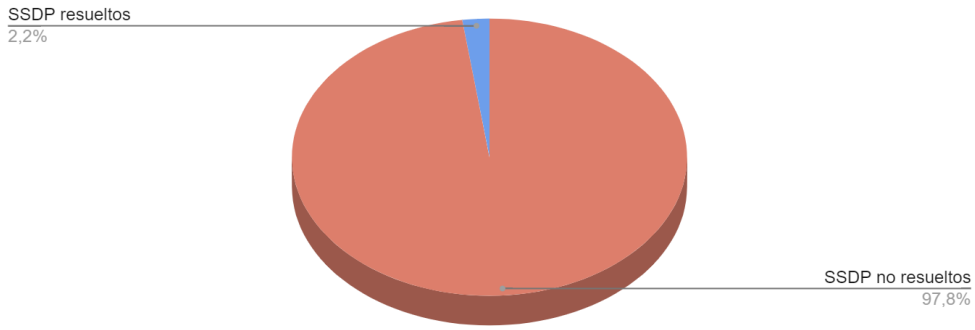
Resultado de las acciones

Las acciones se dirigieron a mitigar las vulnerabilidades encontradas. Como parte de este trabajo se realizó una presentación contando la iniciativa y los resultados preliminares, preservando la confidencialidad de la información en lo que hace a la identidad de las organizaciones, en el First Symposium realizado en el marco de LACNIC 36.

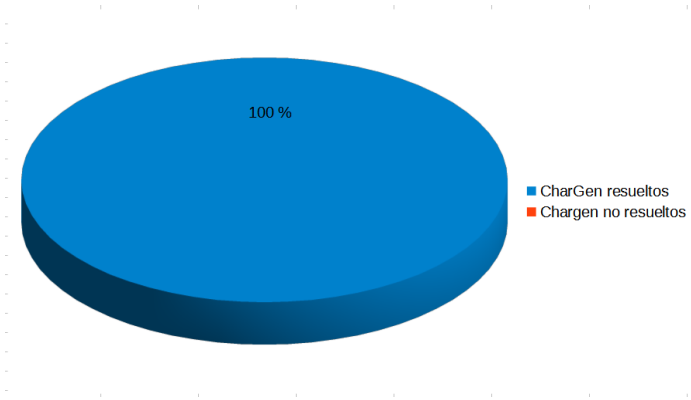
De las doce organizaciones contactadas, solo dos respondieron e interactuaron con el equipo para mitigar las vulnerabilidades reportadas.



En el siguiente gráfico se puede visualizar el porcentaje de casos resueltos que corresponden a una de las organizaciones que dio respuesta y llevó a cabo acciones que mitigaron las vulnerabilidades reportadas referentes al protocolo SSDP.



La otra organización que respondió, como puede observarse en el siguiente gráfico, mitigó la totalidad de las vulnerabilidades de tipo CharGen reportadas.



Si bien solo algunas organizaciones respondieron e interactuaron con el equipo a partir de nuestros reportes, al concentrarse gran porcentaje de los problemas en pocos ASN, se logró tener impacto en la mitigación del problema.

Una de las organizaciones a las que se reportó accionó en favor de la mitigación del problema CharGen, incluso solicitando que hiciéramos un nuevo chequeo. Esto nos permitió corroborar que se habían mitigado las vulnerabilidades reportadas. Como consecuencia, el país al que pertenece esa organización dejó de aparecer en los reportes públicos de Shadowserver sobre CharGen. El estudio considera ese resultado como un caso de éxito.

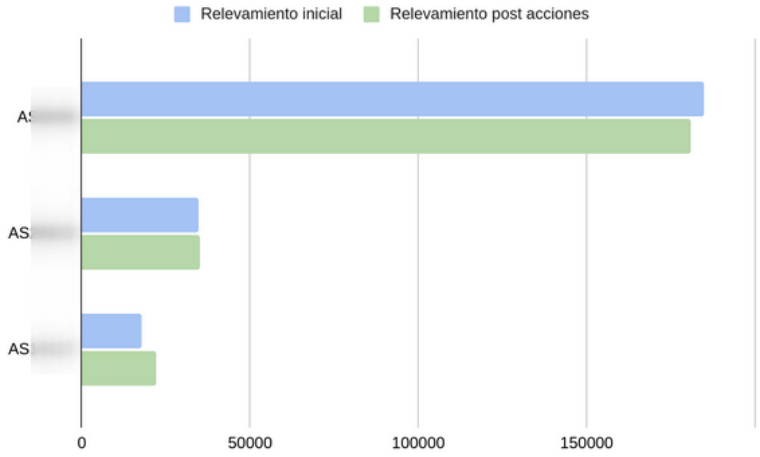
Por último, se relevaron distintos protocolos analizados durante la investigación después de las acciones realizadas.

Sobre las problemáticas en el protocolo SSDP

● La organización con la que coordinamos acciones para explicar la problemática mejoró sensiblemente en relación con la cantidad de dispositivos expuestos. Dado que no informaron sobre sus acciones, no podemos asegurar si esa mejora responde a acciones de mitigación realizadas.

● En otra organización, también se observó un incremento de mejora en la misma magnitud.

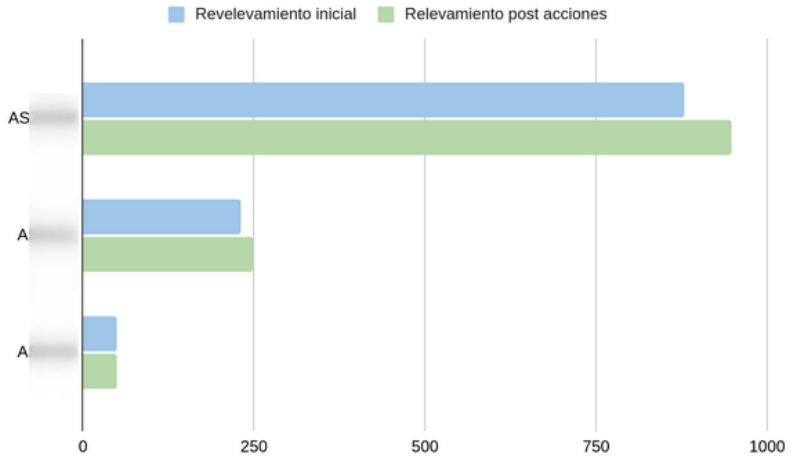
En el siguiente gráfico se reflejan las variaciones de las organizaciones seleccionadas:



Sobre las problemáticas en el protocolo NTP tipo NTPMonitor

● En lo referido al problema de **NTPMonitor**, se observaron cambios levemente desfavorables.

En el siguiente gráfico se reflejan las variaciones de las organizaciones seleccionadas:

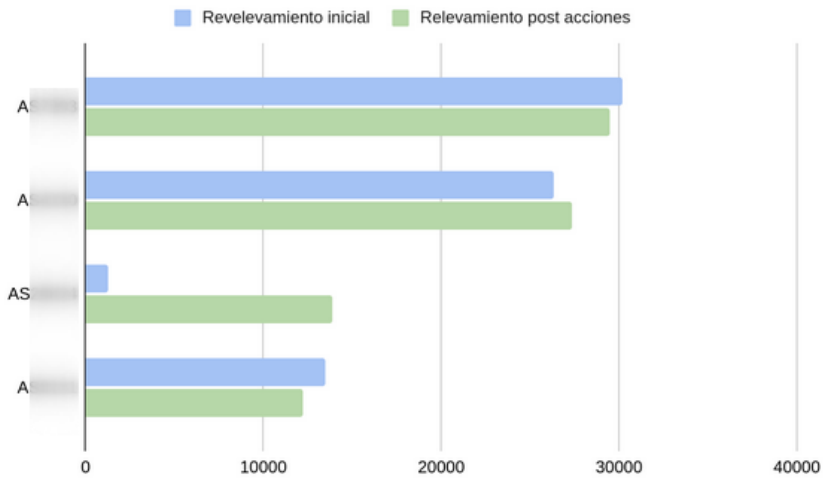


Sobre las problemáticas en el protocolo NTP tipo NTPVersion

● En lo referido al problema **NTPVersion** se observó que, si bien algunas de las organizaciones contactadas no respondieron formalmente a los reportes realizados, dos de ellas mejoraron respecto de la cantidad de dispositivos **NTPVersion** expuestos a Internet.

● Por otro lado, en el Top 4 se observó la aparición de una organización que en el relevamiento inicial tenía una cantidad despreciable de dispositivos **NTPVersion** expuestos a Internet.

En el siguiente gráfico se reflejan las variaciones de las organizaciones seleccionadas incluyendo la nueva organización observada en el relevamiento final:

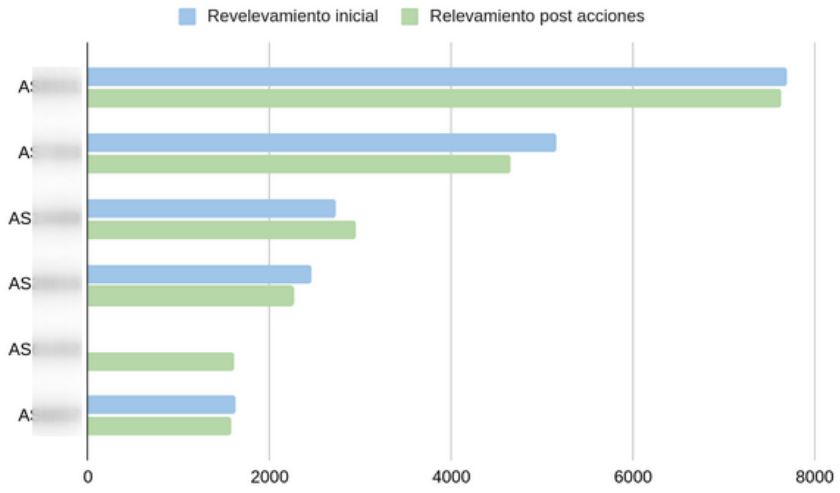


Sobre las problemáticas en el protocolo DNS tipo *open resolver*

En lo referido a la problemática asociada al DNS, debido a la exposición a Internet de servidores que funcionan como *open resolvers*, se observaron mejoras considerables en dos de las cinco organizaciones a las que se informó sobre la situación.

Al igual que en el caso de NTPVersion, se observó la aparición en el Top 8 de una organización que en el relevamiento inicial tenía una baja cantidad de dispositivos DNS OpenResolver expuestos a Internet.

En el siguiente gráfico se reflejan las variaciones de las organizaciones seleccionadas, incluyendo la nueva organización observada en el relevamiento final:

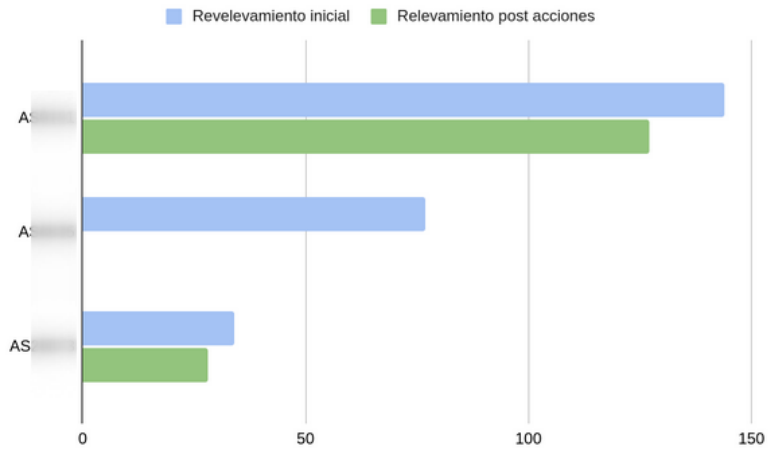


Sobre las problemáticas en el protocolo CharGen

Como se mencionó, pudimos trabajar coordinadamente con uno de los miembros de LACNIC para mitigar el 100% de los servicios CharGen expuestos a Internet en su ASN.

Si bien el resto de las organizaciones contactadas no respondieron formalmente a los reportes realizados, pudimos observar que en estas los servicios de CharGen expuestos se vieron reducidos levemente.

En el siguiente gráfico se reflejan las variaciones de las organizaciones seleccionadas.



Conclusiones

El estudio cumplió su objetivo, ya que se pudieron mitigar vulnerabilidades en la región, lo cual mejora el nivel de seguridad de Internet. Asimismo, la metodología usada propició la interacción entre el CSIRT de LACNIC y sus asociados en temas de seguridad, fortaleciendo el rol del equipo para compartir herramientas que permitan a las organizaciones miembros de LACNIC la prestación de un mejor servicio.

En el relevamiento final se pudo observar la aparición de nuevas organizaciones con un gran volumen de vulnerabilidades que no estaban presentes en relevamientos previos. Esto refleja que acciones como las promovidas durante este estudio son siempre necesarias, ya que aparecen otros actores y, con ellos, idénticas o nuevas situaciones de ciberseguridad.

Se propone realizar un webinar donde se explique la problemática, se ofrezca la colaboración para mitigar las vulnerabilidades asociadas y se discutan acciones posibles para mejorar el nivel de seguridad de la región.

Recomendamos también a LACNIC CSIRT impulsar más proyectos de este tipo para estudiar problemas de seguridad en la región. Por lo general, suelen estar concentrados en unas pocas organizaciones, por lo que trabajar mancomunadamente ayuda a mitigarlos.

Por último, creemos importante difundir en la comunidad servicios como los provistos por Shadowserver. La exposición que estas fuentes de información realizan no solo ayuda a generar conciencia sobre la importancia de la ciberseguridad en las organizaciones, sino también a pensar en la necesidad de tener un CSIRT que aborde estas problemáticas.

Referencias

[1]_https://us-cert.cisa.gov/ncas/alerts/TA14-017A

[2]_https://christian-rossow.de/articles/Amplification_DDoS.php

[3]_https://us-cert.cisa.gov/ncas/alerts/TA14-017A

[4]_https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html

[5]_https://sensorstechforum.com/es/ws-discovery-protocol-ddos/]

[6]_https://www.cloudflare.com/es-es/learning/ddos/memcached-ddos-attack/]

[7]_https://blogs.akamai.com/2018/02/memcached-udp-reflection-attacks.html]

[8]_https://www.akamai.com/us/en/resources/our-thinking/threat-advisories/ddos-reflection-attack-memcached-udp.jsp]

[9]_https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/fbi-private-industry-notification-20200721-002.pdf

[10]_https://www.variot.eu/2020/09/01/scanning-for-accessible-coap-devices/

[11]_https://www.shadowserver.org/news/accessible-coap-report-scanning-for-exposed-constrained-application-protocol-services/

[12]_https://scan.shadowserver.org/

[13]_[https://www.shadowserver.org/news/the-scannings-will-continue-until-the-Internet-improves/

[14]_https://www.shodan.io/

[15]_https://search.censys.io/