DNS IPv4 Open Resolvers Hosted on LACNIC-Managed Number Resources

Contents

Executive Summary

LACNIC CSIRT and CEDIA CSIRT conducted a study to identify open DNS servers associated with an IPv4 address in order to inform the members who were assigned these resources of the situation, suggest alternatives to correct the configuration of their servers, and try to significantly reduce the number of open resolvers in our region. In addition, various means of communication were used to asses their effectiveness.

Open resolvers represent a latent security risk for Internet infrastructure, as these are servers configured in such a way that they can be used to attack third-party infrastructure and carry out denial-of-service attacks.

As far back as March 2013, US-CERT issued TA13-088A,[1] an alert that warns of the problem and proposes mitigation measures.

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

Introduction

Exposed IPv4 endpoints continue to be the most common attack vector to exploit service vulnerabilities. Most attacks are currently executed through vulnerable services running under this protocol.

The use of the IPv4 protocol is also an advantage for CSIRTs, as it is a well-known, controlled universe where it is relatively quick to check for these faults. There are very efficient tools available that can find open ports in the IPv4 space (< 2^32 IP addresses) in just a few minutes, and even more easily when this space is reduced to the resources managed by a specific RIR.

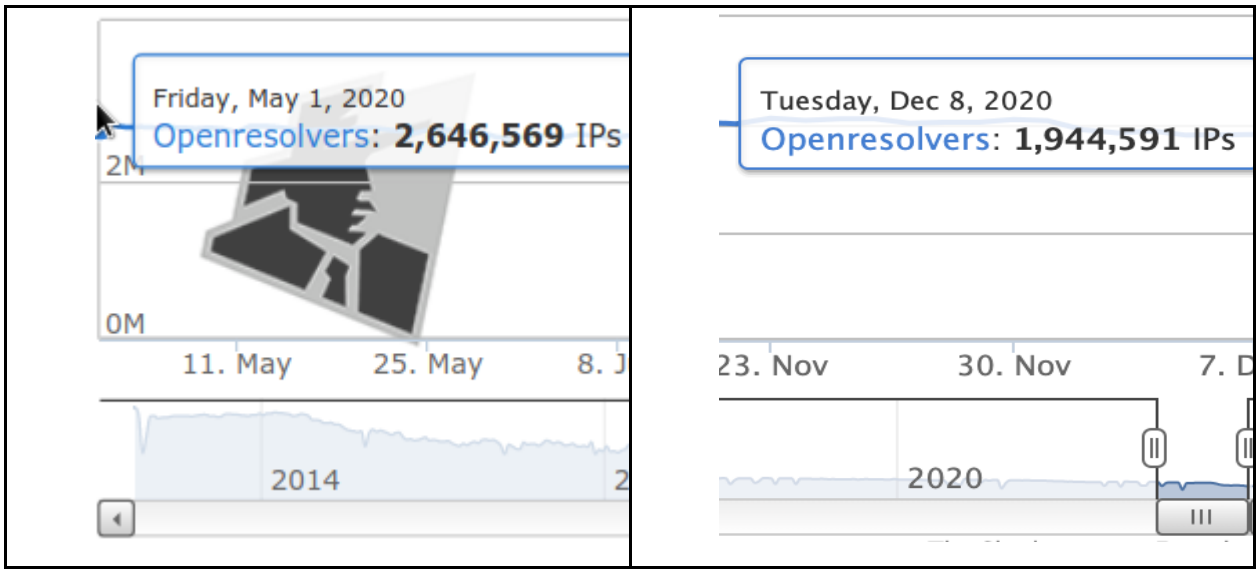
In line with the stated goal of the project, we attempted to locate and report DNS servers that were acting as open resolvers. An open resolver is a DNS server that replies to queries that originate in any network, regardless of whether it is a third-party or its own home network.

An open resolver is a threat to Internet security and stability, as it allows potentially harmful activities to be carried out. These take the well-known form of amplification attacks based on the UDP protocol, where the answer to a query sends back large amounts of information to the chosen victim. In the case of an open resolver, an attacker sends a small query with a fake origin address and a type of record that produces a very large response (e.g., TXT, ANY or queries with DNSSEC extensions).

Overall Situation

According to data obtained from ShadowServer,[2] the number of open resolvers detected worldwide in December 2020 decreased compared to the month of May. However, nearly two million DNS servers — a very high number — remain open and represent a potential threat to the various systems.

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



Impact

Open DNS servers affect those who receive the attack as well as providers and users in different ways. Examples of their impact include:

- **Reputation**: The reputation of the person responsible for the network where the open resolver is hosted may be affected, as the presence of an open resolver may be perceived as careless management of their services.
- **Traffic quality**: The network generates unnecessary traffic which might be avoided, as it affects legitimate traffic and/or the systems that handle network traffic.

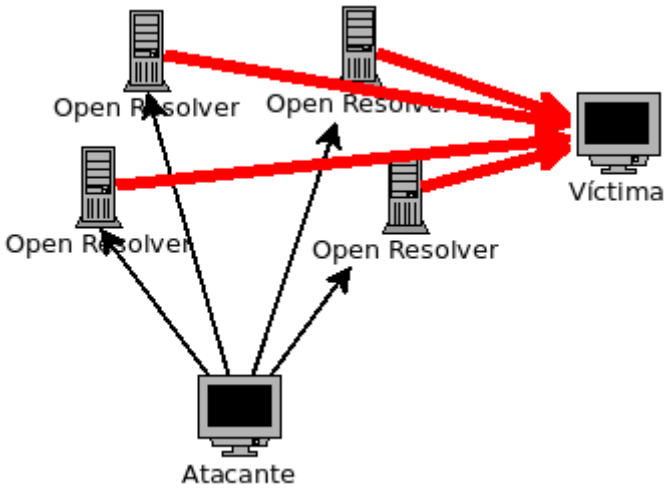
In many cases, the organizations involved are not aware of the existence of this security problem in their network and, therefore, take no action to prevent or solve the problem.

Notifying the problem helps the organization to work on correcting the issue or, at least, to become aware of its existence. If the organization does not have the resources needed to correct the problem, the notification will provide them with a justification to procure the necessary resources.

Packet Flooding Denial-of-Service Attack

The image below shows the *modus operandi* of a packet flooding denial-of-service attack. The attacker sends the same query to different open resolvers, but does so using the victim's address as their origin. The queries are very small in size and consume very little of the attacker's resources, but the victim — who receives

replies from all the open resolvers — will feel the impact of an enormous amount of (unsolicited) information which will undoubtedly deplete their resources.



Mechanisms to Detect Open Resolvers

The process for detecting an open resolver consists of determining whether a response is obtained when port 53/UDP of a certain IP address is queried. If a response is obtained, it is an open resolver.

However, querying all the IP addresses of all existing networks would be very expensive, even if the queries were limited to theIPv4 resources managed by LACNIC. This is the reason why a recursive DNS query is sent only to those IP addresses with port 53/UDP open.

It should also be noted that this process merely provides a snapshot of the situation at the time of the query. Replies may vary greatly from query to query, as they depend on factors such as timeouts, devices that have been shut down, unexpected replies, and blocking by IPS's/firewalls. Thus, it is important to permanently monitor open resolvers in order to find those that may not have appeared in prior searches.

Tools and Data Sources

The first step of this research involved assessing various techniques, tools and data sources related to the topic.

Tools

Dig / Host

These tools allow checking whether a specific IP address responds to a query to the DNS service. To do so, we must specify the IP address to be checked. Address ranges are not supported, only the IP address they will query. If the IP address replies, this can be considered an open resolver; if it does not reply, it means that there is no evidence that it is an open resolver.

Both are adequate for the purpose of the project. We selected Dig for our validations.

NMAP

NMAP is a very well-known tool that allows testing an address range or network to find open ports.

Masscanner

Similar to NMAP. In fact, it uses practically the same command-line flags. It allows the user to input a list of networks or IP addresses and ports and provides a list with the results of the test.

Data Sources

Shodan

We queried the well-known Shodan database to obtain lists of open DNS resolvers in the region and found two limitations:

- The list is not updated daily. It is possible to obtain a report of open ports 53, although this does not mean that they are open resolvers.
- The resulting list is not updated in a predictable manner over time.

Shadowserver[3]

We contacted Shadowserver. Although we expected a very similar set of results, these were, in fact, quite different to the results we obtained from our measurements. In some cases, open resolvers were found that were not included in the Shadowserver list; in others, the opposite occurred. This difference may be due to various factors, such the RIR to which the network belongs (not always LACNIC), the time at which the checks were performed, the potential implementation of IP ACLs to prevent access from specific networks, long response times, etc.

Eventually, we thought of consolidating or contrasting the data from both sources. However, because the universe of IP addresses used by Shadowserver was unknown to us, this could have contaminated our results instead of enriching them.

LACNIC's delegated-extended File

For the reasons above, we decided to use the information collected directly from LACNIC's delegated-extended file.

Procedure

The following is a description of the procedure used to scan LACNIC-managed IPv4 address blocks.

1. The LACNIC-extended file was downloaded from LACNIC's FTP server. This file contains the subnets assigned in the LACNIC service region.
2. The results were converted to CIDR format.
3. A supernetting of these ranges was performed and this list was used to feed *masscanner*.
4. Using *masscanner*, the list was searched for open 53/UDP ports.
5. Using the *dig* command, the IP addresses with 53/UDP port open were searched for domain servers that responded to a query that was specific and unique to a domain under the control of CEDIA: test-csirt.cedia.org.ec (TXT).
6. A list was obtained of the points of contact for the resources for which a positive result was obtained in the previous step.
7. The resources managed by the NIRs were separated.

---

[3] ‹https://www.shadowserver.org/›

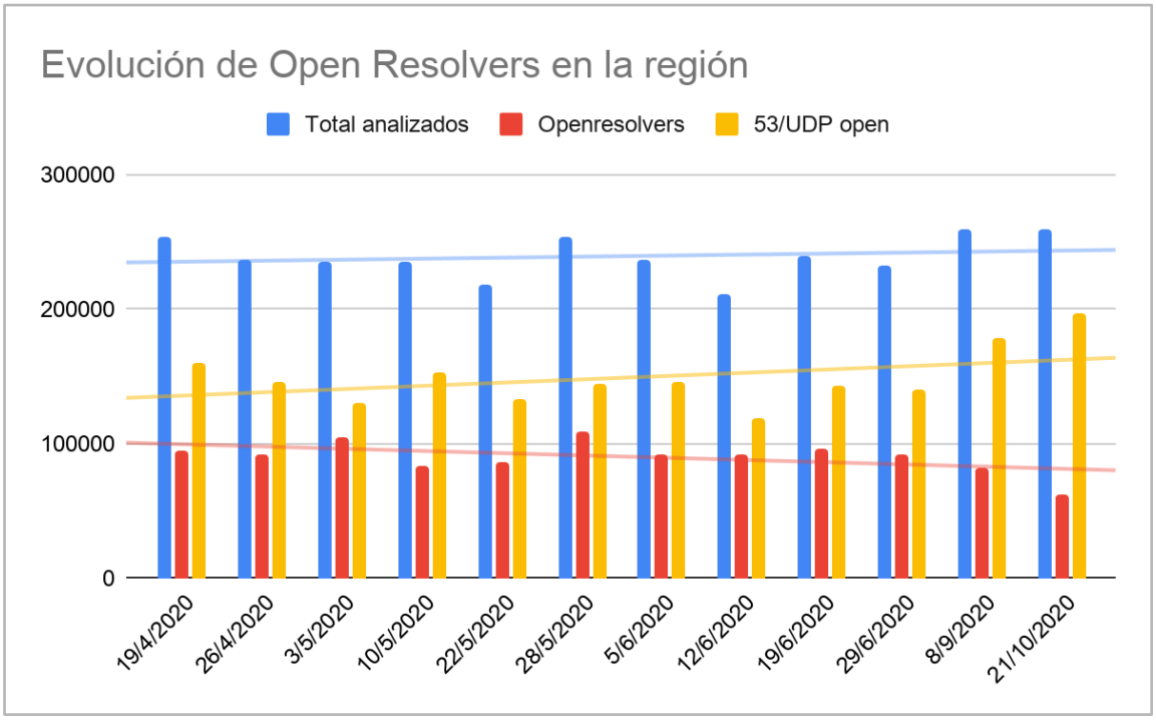
8. Notifications were organized and sent through three different channels (email, direct contact with the person responsible for the resources, and via the MiLACNIC security module).
9. These notifications also contained suggested solutions (see Appendix 1). The procedure described above was refined and performed on three separate occasions.

For comparison purposes, the first IP addresses classified as open resolvers were kept within the dataset under analysis.

Number of Open Resolvers Detected During the Analysis

Of the total number of IP addresses that were analyzed, only those with port 53/UDP open and which replied to DNS resolution queries were confirmed as open resolvers. The IP addresses that did not reply to the queries were recorded simply as port 53/UDP open.

The chart below shows the evolution of the number of open resolvers during the period of the study. As we can see, this number decreased.



Analysis and Evaluation of Actions for Reporting Open DNS Resolvers

Contacts were made through three different channels: email, direct contact and MiLACNIC.

Of the group of IP addresses linked to an open DNS service, those managed by NIRs NIC.Mx and NIC.Br were separated and the rest of the list was divided into three subgroups. Each of these was assigned one of the following communication channels:

1. **Email:** An email was sent to the contacts registered for each IP address in Argentina, Chile and Colombia.
2. **Direct contact:** Known contacts at the five organizations with the highest number of open resolvers were contacted in different ways. These were not necessarily the contacts registered for each IP address. To do so, we used social techniques, i.e., we called persons we knew at these organizations.
3. **MiLACNIC:** A notification was sent via the MiLACNIC portal (excluding organizations in Brazil, Mexico, Argentina, Chile and Colombia, as they had already been included in one of the subgroups above).

Results Related to the Communication Channels

The table below shows the number of resources identified as open resolvers in each round along with the communication channel that was used in each case.

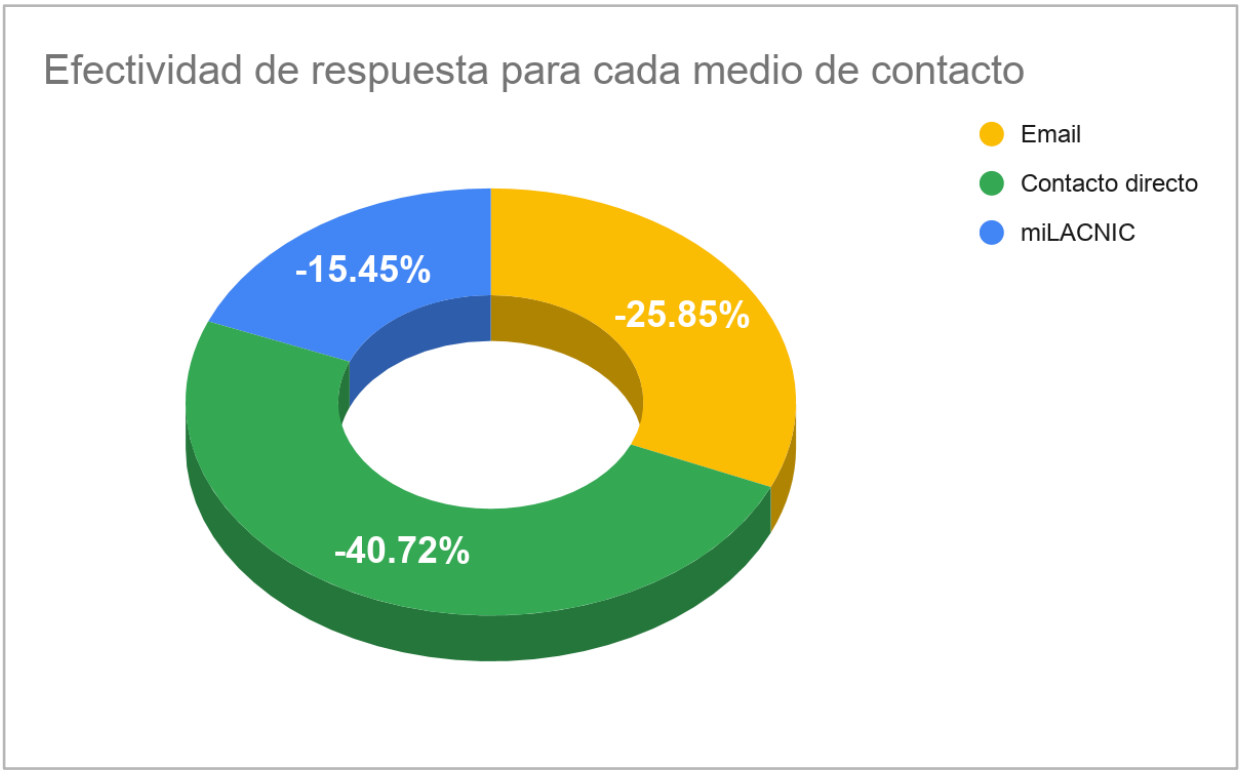
Communication channel	29 June 2020 1st round	08 September 2020 2nd round	21 October 2020 Last round	Difference (%) 1st vs. last
Email	19084	10920	14151	-25.85
Direct contact	5545	3191	3287	-40.72
MiLACNIC	11436	7317	9669	-15.45
Total	36065	21428	27107	-24.84

It is interesting to share some comments related to these results.

- The responses received via email included messages such as the following:
  - Notes thanking for the notification and acknowledging that corrective action would be taken.
  - Notes informing that the suggested actions had been implemented and that the problem had been fixed.
  - Requests for additional help.
- More than 12% of the messages sent via email during the first round bounced because the contact information in WHOIS was incorrect.

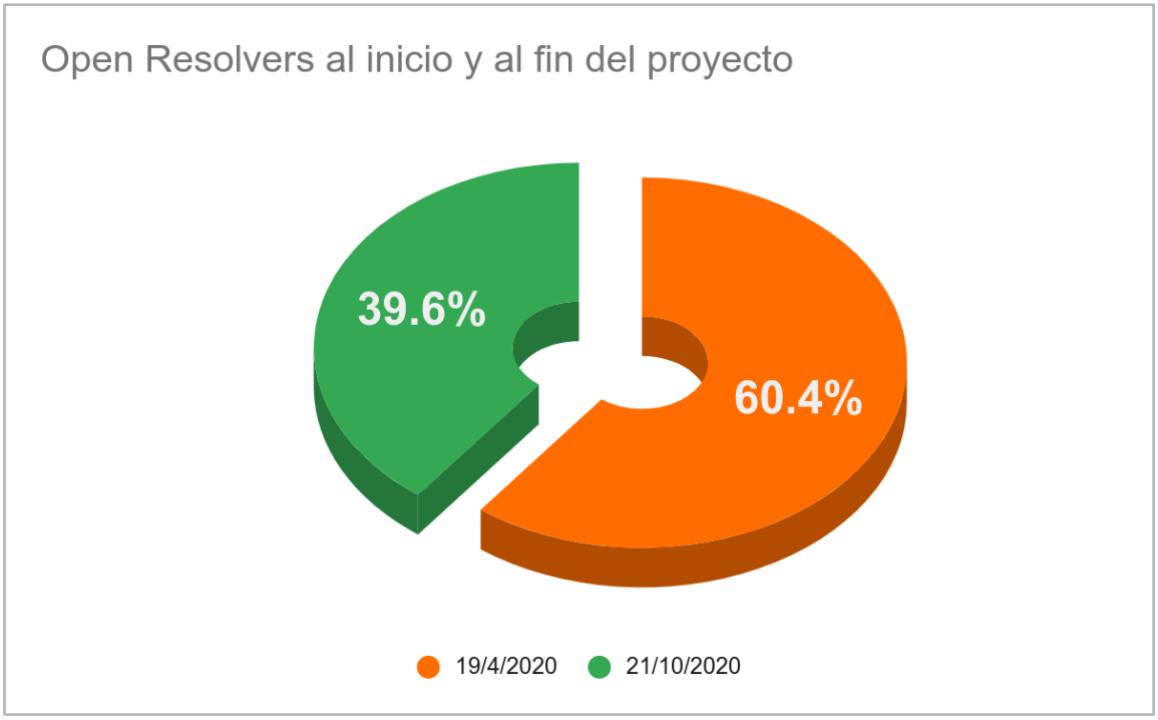
- Although during the first round only one response was obtained through direct contact, results show that actions were implemented, as there was a drastic decrease in the number of open resolvers.
- No feedback was received via MiLACNIC.

The chart below compares the different success rates depending on the communication channel that was used. Here, success is defined as a server that replied to the query that was sent.



Conclusions

Overall, we believe that the result was successful, as we managed to significantly decrease the number of open DNS servers, as shown in the chart below.



Email was identified as the most effective channel to alert the target community about existing security vulnerabilities in their systems and to help correct them.

Along the same lines, it was concluded that there are many technical or abuse email contacts to which it is not possible to send reports for various reasons. Organizations should keep these email contacts operational and up-to-date so they can receive reports on any security incident that may arise.

To decrease the number of open resolvers in the region, it is necessary to automate the procedure for their detection and notification to the persons responsible for the resources. Reports should be sent to the organizations using a combination of email and the MiLACNIC security module.