# Study of Internet Resources in the LACNIC Service Region that Use UDP and Enable DDoS Attacks

(Ref. SSR Study 2021)
Final Report

Authors: Paula Venosa, Nicolas Macia, Guillermo Pereyra
Coordination/Revision: Graciela Martínez
Edition: Carolina Badano, María Gayo, Martín Mañana
Project: Strengthening Regional Internet Infrastructure
Department: CSIRT LACNIC

lacnic
www.lacnic.net

*!*

## *Executive Summary*

This study managed to identify and mitigate vulnerabilities in the protocols used in the LACNIC service region to conduct denial of service attacks, consequently improving the level of Internet security.

It also promoted interaction between LACNIC CSIRT and its members on security issues, strengthening LACNIC CSIRT's role in sharing tools that will allow LACNIC member organizations to provide better services.

The study identified the vectors used in DDoS attacks, including a list of protocols over UDP that can amplify the magnitude of an attack. It also allowed LACNIC CSIRT to work directly with the affected organizations to help them reduce their risks.

## *Abstract*

This report describes the study conducted to survey the presence of scalable User Datagram Protocol (UDP) services which can be used to perform distributed denial of service (DDoS) attacks in Latin America and the Caribbean.

It includes the methodology applied for the study, presents the results of an initial survey, and offers a first series of recommended actions to mitigate these attacks. It also includes a subsequent situation analysis after the implementation of these actions.

## *Purpose*

To improve the cybersecurity levels of the IP resources managed by LACNIC, contributing to Internet stability and resilience by minimizing the potential use of UDP protocols in DDoS attacks.

## *Motivation*

Amplification DDoS attacks are one of the most common types of attacks experienced by organizations today. They take advantage of two design flaws in network protocols:

- The information in the IP header is not authenticated.

- UDP has no handshaking dialogues.

These attacks have a major impact on the community, as they afford attackers significant advantages. Firstly, by using vulnerable services as traffic reflectors, these attacks inherently hide the attacker's address, thereby making it difficult to determine the origin of the attack and potential mitigation actions.

Secondly, small requests to different reflectors usually suffice to trigger large responses. This can be used to generate and direct large volumes of traffic to a targeted victim organization. Depending on the protocol exploited by a DDoS attack, amplification factors of 100x or more can be achieved [1] [2].

This study stresses the need to raise awareness in order to minimize the number of devices connected to the Internet which, due to a lack of knowledge on the part of their administrators, may be used to launch DDoS attacks.

## *Preliminary Analysis of the Problem*

### *Introduction*

A distributed denial of service (DDoS) attack is launched from different origins for the purpose of rendering inaccessible an Internet resource, service, or network. DDoS attacks can affect the victim organization's resources for as long as the attacker desires. Depending on the volume of traffic received by the target, an attack can affect not only the victim organization, but also its Internet provider.

One way to conduct these attacks is to leverage the presence of reflective and amplifiable services exposed to the Internet. Reflective services are services that do not require handshaking prior to exchanging data. It follows from this that any service that uses UDP as transport protocol can fall into this category.

The other requirement is that, in addition to being reflective, the service must be amplifiable. Amplifiable services are services which provide a response that is not much larger than the specific requirement they receive. This difference is known as the amplification factor.

### *Potentially Amplifiable Protocols*

Several Internet protocols fall into the reflective and amplifiable category. Some of these protocols, such as CHARGEN, should not be exposed to the Internet. Others, such as NTP, may create vulnerabilities in the servers where they are implemented.

Finally, it should be noted that improper configurations, for example in NTP or DNS, may cause reflective services to be exposed and lead to undesirable amplifications.

US-CERT National Cyber Awareness System Alert TA14-017A [3] identifies several protocols that rely on UDP as potential DDoS attack vectors. It reports the protocols, their amplification factor, and the associated vulnerable command.

Originally published in 2014, this Alert has been updated several times and new vulnerable protocols have been incorporated which may potentially be exploited or which were used in DDoS attacks that generated large volumes of traffic [4] [5] [6] [7] [8].

| 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 | — |

Additionally, in 2020, a notification issued by the FBI as well as several websites dedicated to the analysis of DDoS attacks mentioned additional protocols to those previously noted by alert TA14-017A. These include CoAP, a web transfer protocol designed for constrained nodes and networks and with the potential for use in Internet of Things (IoT) applications [9] [10] [11].

In the future, this list of reflective and amplifiable protocols may change, as additional vulnerable protocols may appear or new ways of using existing protocols to cause hitherto unexpected amplifications may be discovered.

*Information Sources*

There are different ways to detect devices that expose reflective and amplifiable protocols to the Internet. The best way to determine the existence of a vulnerable protocol is to connect to every possible IP resource and attempt to perform an innocuous query using that protocol. In this sense, Shadowserver Foundation's SCANNING Project is worth noting. Among other things, this project attempts to identify the presence of Internet resources implementing reflective and amplifiable protocols [12] [13].

Another option is to use open information sources that provide threat intelligence or OSINT. Examples of this type of open information sources include SHODAN and CENSYS, which can be used to detect vulnerable amplifiable services [14] [15].

However, just because a protocol is exposed does not necessarily mean that it is vulnerable and may be exploited. For example, a DNS server is vulnerable if it is configured as an open resolver with no restrictions to its utilization. Therefore, depending on which protocol is being evaluated, it may later be necessary to verify whether the service is vulnerable or not.

*Analysis of the Protocols of Interest to the Study*

While ideally the study would like to eradicate any protocol that is vulnerable to amplification attacks, we selected those which might represent the greatest risk to Internet security and stability. This selection was based on the following:

- Reflective and amplifiable protocols that are known to be used in this type of attacks.
- New vulnerable protocols detected in recent years.
- Each protocol's potential amplification factor.
- The number of potentially vulnerable devices on the Internet.
- Available sources of information.

We began by analyzing the services usually considered the clearest examples of this problem and used Shodan to obtain a quick estimate of the number of devices exposing this service to the Internet. The table below was generated by combining this information with the corresponding amplification factor.

| 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 |

The following observations are based on these results:

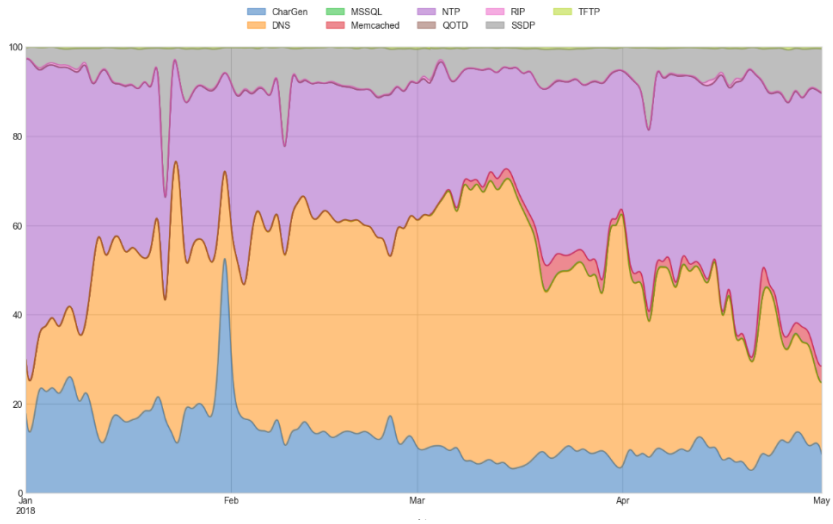
" Not all devices estimated by Shodan are reflective. The following protocols can work both over UDP as well as over TCP: Memcached, DNS, WS-Discovery, CharGen, SNMP, and QOTD.

" Because Shodan does not allow querying protocols that run exclusively over UDP, in principle, we are not sure how many of these can be used to generate a DDoS attack, something that is of interest to this study.

" The protocols reported by Shodan are versionless. This is of interest in the case of SNMP, as 2c is the vulnerable version which allows the GetBulk command to be used reflectively to achieve high amplification factors.

In addition, this analysis used information from different sources in order to compare the risk currently represented by each of these protocols. In this sense, while all the issues are serious, it is worth mentioning that:

" During 2018, a study conducted by a project funded by the European Union [https://sissden.eu/blog/amp2018] and operating a network of honeypots designed for amplification DDoS attacks showed that CharGen, DNS, NTP, and SSDP were the most prevalent attack vectors.

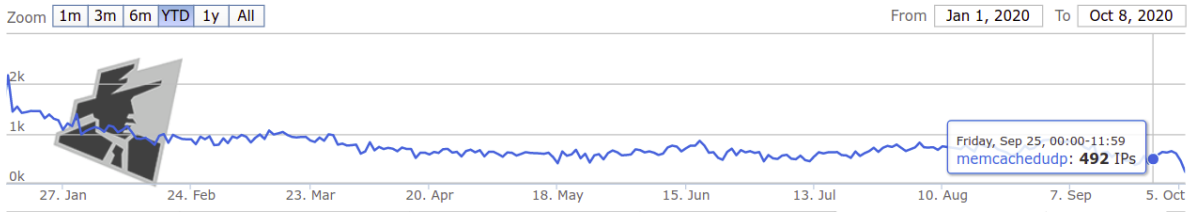



" Public data from the Shadowserver Foundation were analyzed. The Shadowserver Foundation gathers and analyzes data on malicious Internet activity. In particular, public national and global statistics were analyzed for the different protocols that can be used in DDoS attacks.

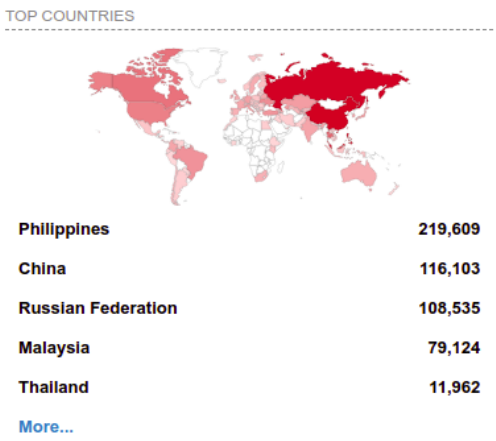
" The Memcached protocol burst onto the reflective and amplifiable services scene in February 2018, when it was used to generate the largest-ever volumetric DDoS attack which led one of Akamai's customers to experience 1.3 TBps of sustained traffic [8]. From that moment on, the issue gained visibility and awareness was raised

among the community. As a result, Shadowserver Foundation now produces statistics that show the number of Memcached servers over UDP on the Internet.


The chart begins at the time of the DDoS attack described above, and a reduction is clearly visible from that moment on. The data available for 2020 — the latest data published by Shadowserver — allow a better understanding of the scale of the number of reflective servers using this protocol:




As for CoAP, a protocol that can be expected to be found on multiple Internet of Things (IoT) devices, the European Union's VARIoT project is trying to classify vulnerable IoT devices exposed to the Internet. VARIoT project outcomes show that the vast majority of accessible devices are found in the Philippines, Russia, and China [10]. This information was also compared with information available through Shodan, which showed that, in the LACNIC service region, the number of devices implementing CoAP is not significant.



Finally, our analysis of the protocols that would be of interest to the study included how to define whether an exposed service was vulnerable. In this sense, for each of the protocols we analyzed, we studied whether the response to a valid request would be enough to determine if the service was vulnerable.

In the case of WS-Discovery, verifying the vulnerability of the exposed service required sending a malformed command. However, valid commands are available for the remaining protocols that allow confirming the vulnerability of a service without jeopardizing its normal operation. In our opinion, including the WS-Discovery protocol in the study would not have been appropriate, as it is impossible to guarantee the security of the tests conducted on this type of devices.

Based on these results, we concluded that an analysis and evaluation of the problem at the regional level would be appropriate, focusing on the detection, awareness, and mitigation of vulnerable instances of services using the NTP, DNS, CharGen, and SSDP protocols.

### *Initial Survey*

During the preliminary phase of the study, the decision was made to analyze and evaluate the problem in our region, focusing on the detection, awareness, and mitigation of vulnerable instances of the NTP, DNS, CharGen, and SSDP protocols.

First, different sources of information were surveyed. Once the information had been gathered, an analysis was conducted and mitigation actions were defined.

#### *Information Sources Used in the Survey*

In addition to conducting our own tests, the study also used information provided by both Shadowserver and Shodan. Shadowserver's SCANNING project[1] was used as our primary source of information as, among other issues, it identifies the presence of Internet resources that implement amplifiable and reflective protocols as discussed in this study.

---

1 https://scan.shadowserver.org/

A significant advantage in using Shadowserver as a source of information is that the project is not limited to scanning the services, but rather assesses whether they are vulnerable and can be used in amplification attacks.

In the case of the CharGen protocol where the mere exposure of the service is enough to consider it vulnerable, Shodan was used as the primary source of information, as we contacted Shodan and were informed about the possibility of searching for instances of the service running over UDP . This search was performed as follows: *«port:19 shodan.module:newline-udp»*.

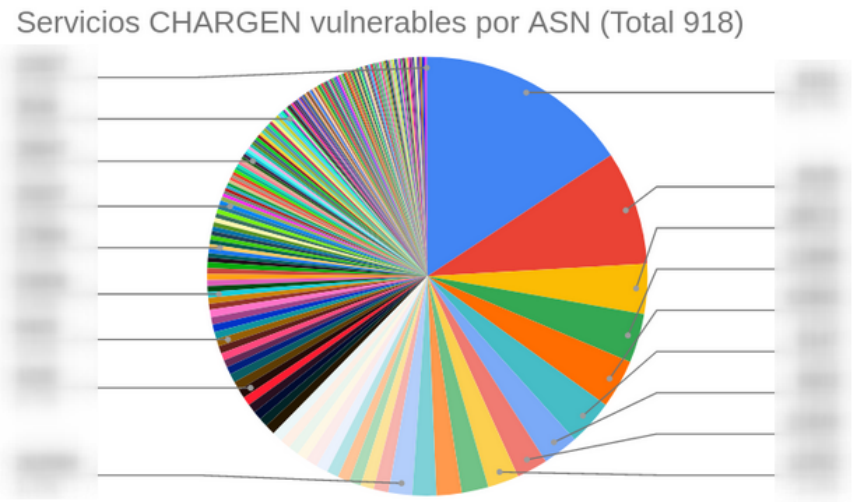
The experience was extremely interesting, as the TCP instances of this service are not vulnerable because TCP is not a reflective protocol (while UDP is).

In addition, manual tests were performed to verify the information provided by the sources listed above. Manual tests were also performed to analyze situations that might potentially raise questions, such as the one observed regarding the SSDP service reported by Shadowserver which detects the presence of the protocol on different UDP ports.

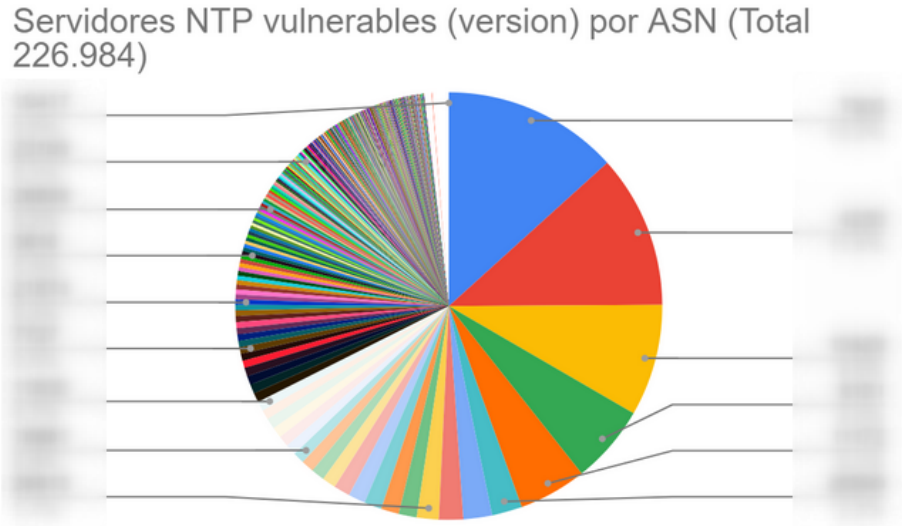
*Preliminary Findings*

We summarized the data of the reports we obtained in different ways, namely, vulnerable servers and services by autonomous system and by country. Considering that summarizing the data by country does not reflect the issues specific to each country but instead relates exclusively to their size, we preferred to analyze the issues related to each protocol by autonomous system.

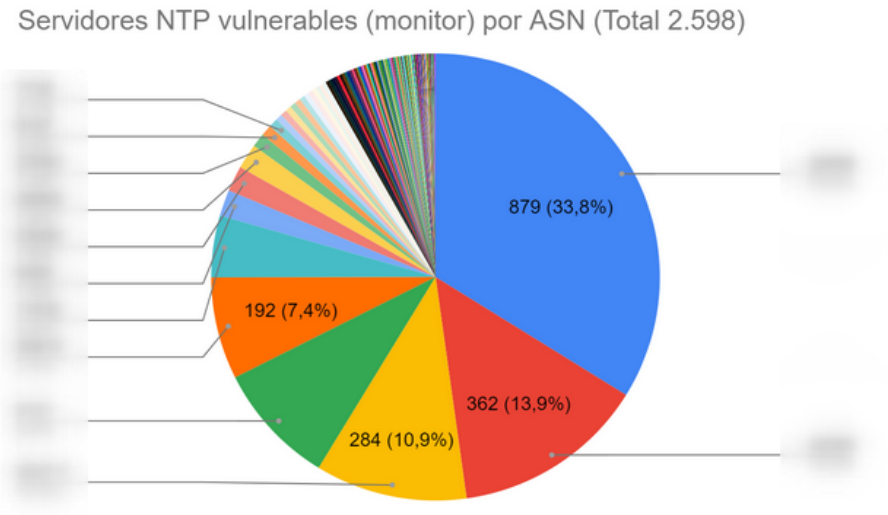
The following chart shows the percentage of vulnerable CharGen services by ASN. A total of 918 vulnerable services were found for the region as a whole.



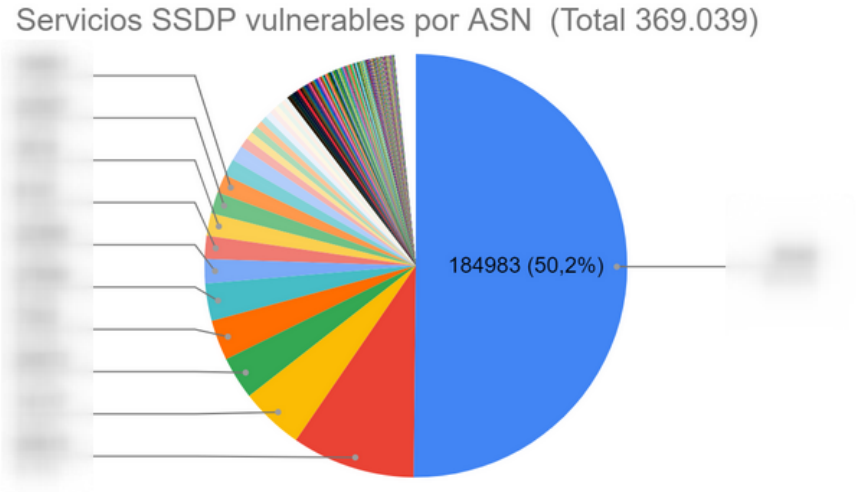

The following chart shows the percentage of NTP servers by ASN that support READVAR (Mode 6) queries. A total of 226,984 vulnerable servers were found for the region as a whole.



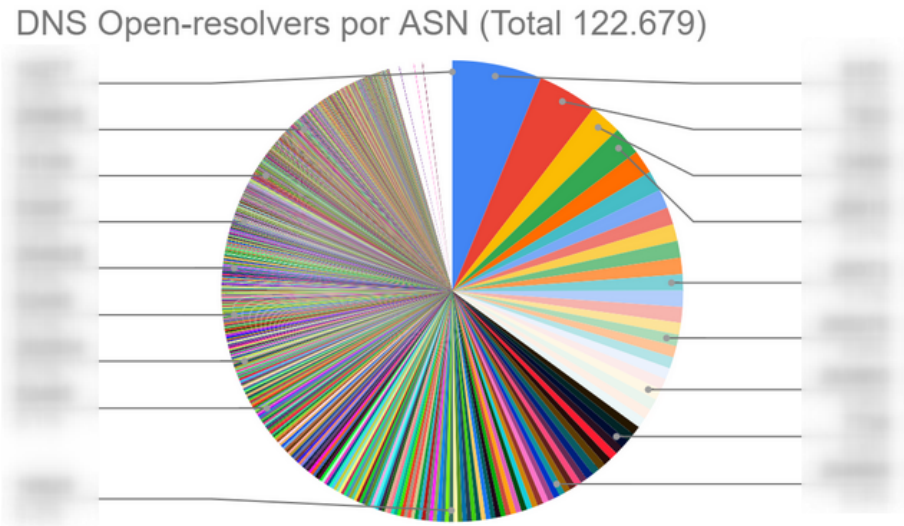

The following chart shows the percentages of NTP servers by ASN that support MONLIST (Mode 7) queries. A total of 2,598 vulnerable servers were found for the region as a whole.




The following chart shows the percentages of vulnerable SSDP services by ASN. A total of 369,039 vulnerable services were found for the region as a whole.




The following chart shows the percentage of open DNS resolvers by ASN. A total of 122,679 open DNS resolvers were found for the region as a whole.




*Analysis*

By processing the information in a graphic format, we were able to design a strategy for reporting the vulnerable targets we detected, thus maximizing the number of vulnerabilities we would be able to manage. The following observations and determinations are based on the charts above:

" Based on the data obtained for the **NTPversion** and **NTPmonitor** protocols, the decision was made to report each type of issue separately so that they could be properly managed.

" In the case of the SSDP protocol, a very large disparity was observed between the autonomous system with the highest number of vulnerable targets and the others. This autonomous system even places the country where the organization is located on Shadowserver's list of Top 20 countries with open SSDP.[2]

" Taking advantage of the fact that a large percentage of the vulnerabilities detected for the CharGen, SSDP, and NTP protocols were concentrated in a just few organizations, the decision was made to report to the three organizations where the highest number of vulnerable targets was found (per protocol), with the following considerations:

# Maximizing the percentage of vulnerabilities that could be managed.

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

# Including organizations from different countries so as to cover different geographic regions in the area serviced by LACNIC and including them in subsequent awareness raising stages.

" In the case of open DNS resolvers, given the uniformity observed in the number of cases detected per organization, the decision was made to report to the five organizations with the highest number of open DNS resolvers, also including organizations from different countries.

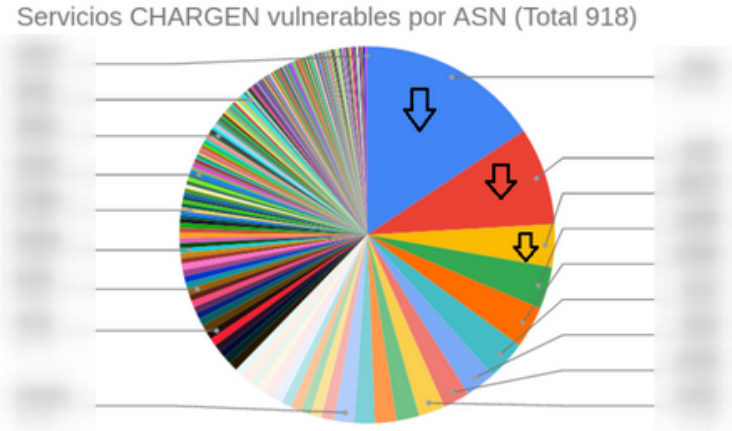
" In the case of the SSDP protocol, it should be noted that Shadowserver reports included devices running on different ports, and that port 1900 was not the port that was used the most.

### *Actions*

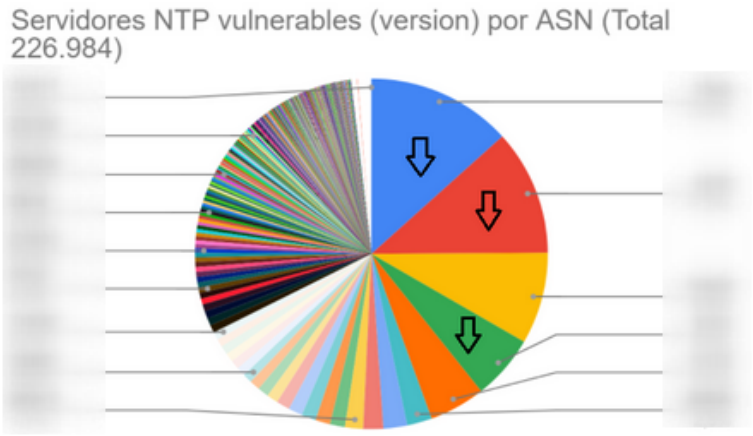
The study included the following actions:

" The organizations for which the vulnerabilities of the different protocols were to be recorded were selected:

**CharGen**

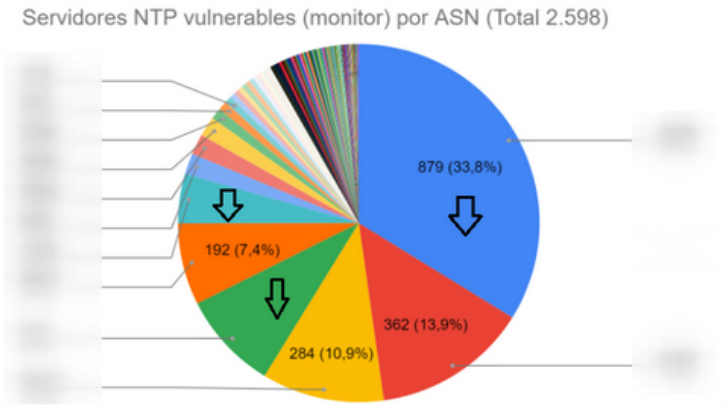



**NTP (version)**



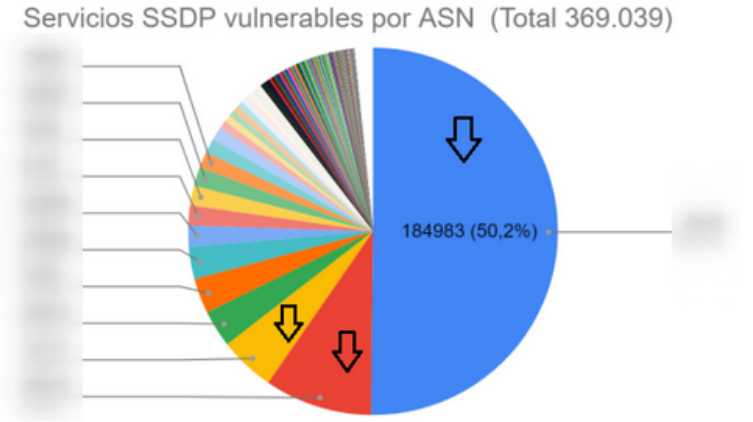

**Note:** The third ASN was not selected. Instead, organizations from three different countries were included to increase the project's coverage for mitigating this vulnerability.

## NTP (monitor)

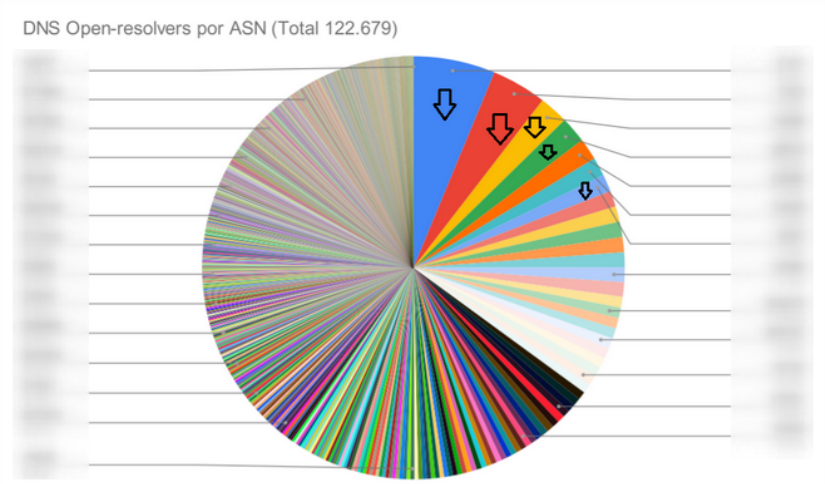



**Note:** The second, third and fifth ASNs were not selected. Instead, organizations from three different countries were included to increase the project's coverage for mitigating this vulnerability.

## SSDP




## DNS




**Note:** The fifth and sixth ASNs were not selected. Instead, organizations from five different countries were included to increase the project's coverage for mitigating this vulnerability.

" A search for valid points of contact for the selected organizations was performed. Together with LACNIC, a search for contacts was performed using the information provided by the WHOIS and RDAP services. Information available from the CSIRTs operating in our community was also used to find alternative points of contact where necessary.

" Twelve organizations from countries in the region were contacted. For one of these organizations, four issues were detected; for others, two.

" The different findings were reported.

" Evidence was produced to inform the affected parties of the detected issues so that they would be aware of their impact.

" Selected LACNIC members for which vulnerable services were detected were contacted. A first message was sent explaining the purpose of the project and asking them to confirm whether they agreed to be contacted. Members were then asked whether they would like to receive specific information regarding the vulnerabilities detected by the project.

Depending on the needs of the organizations we contacted for the purpose of offering our support:

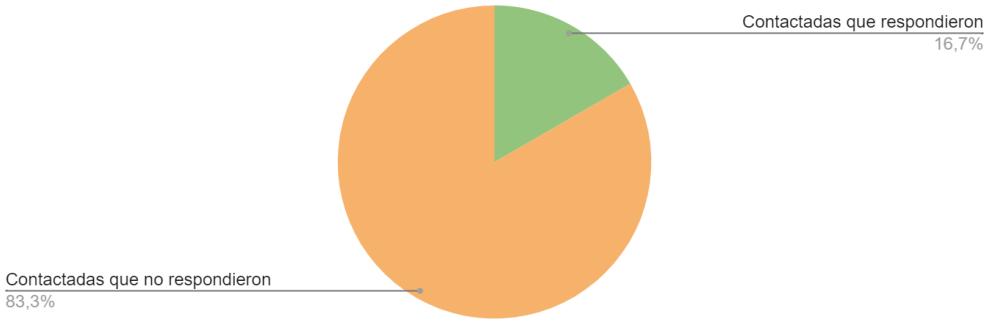
" Meetings were scheduled to collaborate with the affected members to mitigate the vulnerabilities that were detected and thus improve regional security levels.

" Questions and concerns were addressed via email, both to support their mitigation efforts and to verify the correct solution of the reported issues.

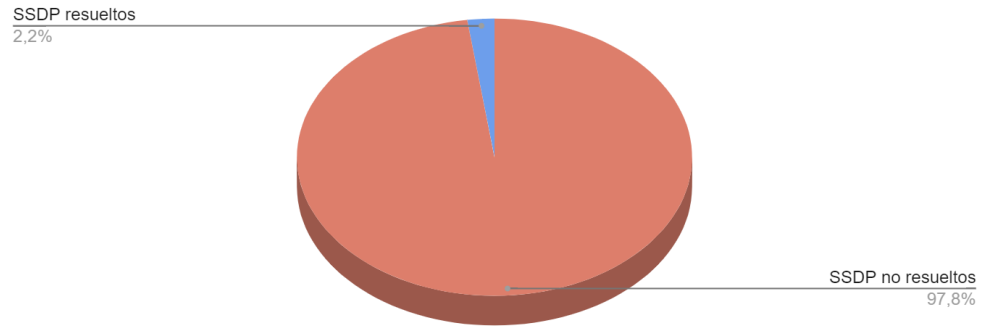
### *Result of the Actions*

The goal of the actions above was to mitigate detected vulnerabilities. Our work included a presentation to explain the initiative and its preliminary results during the FIRST Symposium held within the framework of LACNIC 36. The confidentiality of the identity of the organizations was maintained.

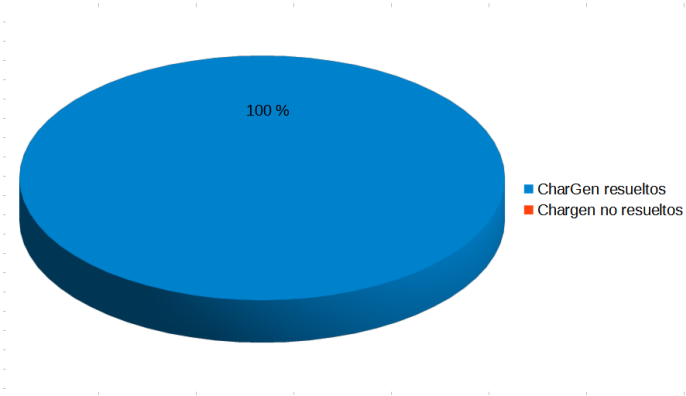
Of the twelve organizations that were contacted, only two replied and interacted with the team to mitigate the reported vulnerabilities.




The following chart shows the percentage of cases that were solved. This number represents the organization that replied and implemented actions to mitigate the reported SSDP protocol related vulnerabilities.




As shown in the following graph, the other organization that replied mitigated all of the reported CharGen vulnerabilities.




Although only a few organizations replied and interacted with the team, the fact that a large part of the issues were concentrated in a few ASNs made it possible to have an impact on mitigating the problem.

One of the organizations to which a report was sent implemented actions to mitigate the CharGen issue, even requesting that we perform a new check. This allowed us to verify that the reported vulnerabilities had been mitigated. As a result, the country where that organization is based no longer appears in Shadowserver's public reports on CharGen. We consider this result to be a success story.!

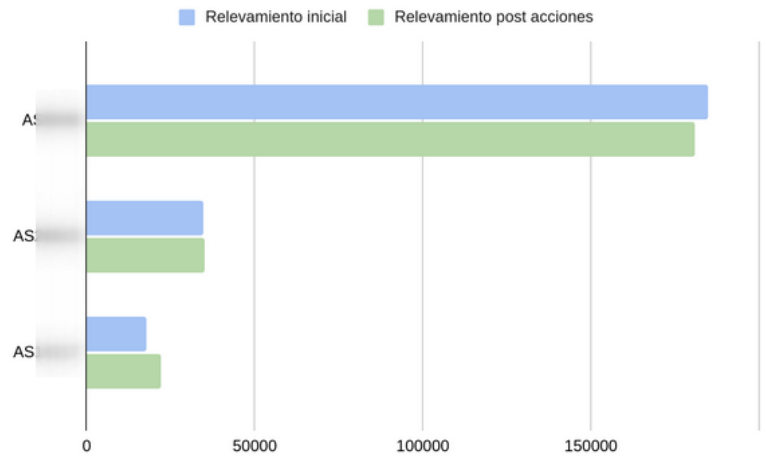
Finally, different protocols analyzed during the study were surveyed after implementing the actions above.

**About the Issues Relating to the SSDP Protocol**

" The organization with which we coordinated actions to explain the problem significantly decreased their number of exposed devices. Since they did not report their own actions, we cannot be sure if this improvement was the result of mitigation actions.

" A similar improvement was observed in another organization.

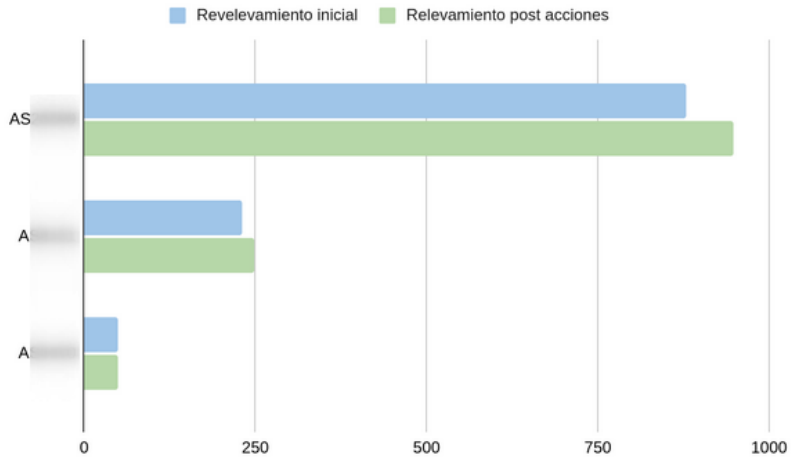
The following chart reflects the variations experienced by the selected organizations:




**About the Issues Relating to the NTPMonitor-Type NTP Protocol**

" Slightly negative changes were observed in relation to the number of issues relating to **NTPMonitor**.

The following chart reflects the variations experienced by the selected organizations:

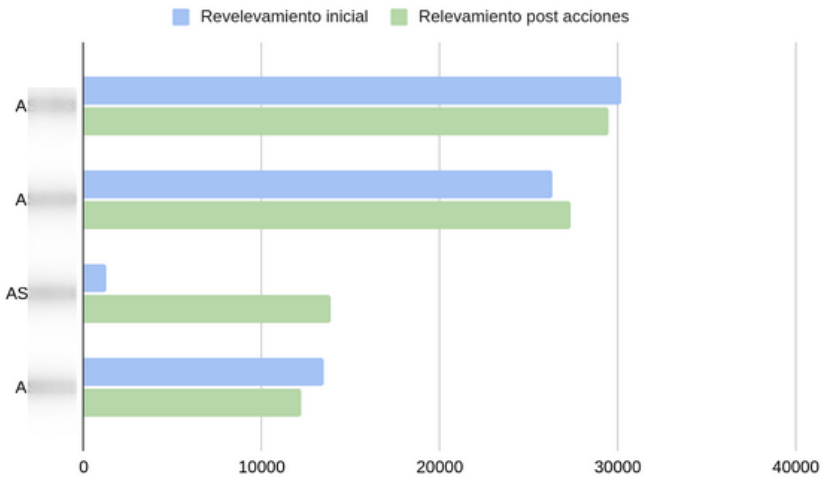



**About the Issues Relating to the NTPVersion-Type NTP Protocol**

" As for the issues relating to NTPVersion, we noted that, although some of the organizations we contacted did not formally reply to our reports, two of them improved in terms of the number of **NTPVersion** devices exposed to the Internet.

" On the other hand, one organization which had an insignificant number of **NTPVersion** devices exposed to the Internet when the initial survey was conducted later appeared among the Top 4.

The following chart reflects the variations experienced by the selected organizations, including the organization observed during the final survey:

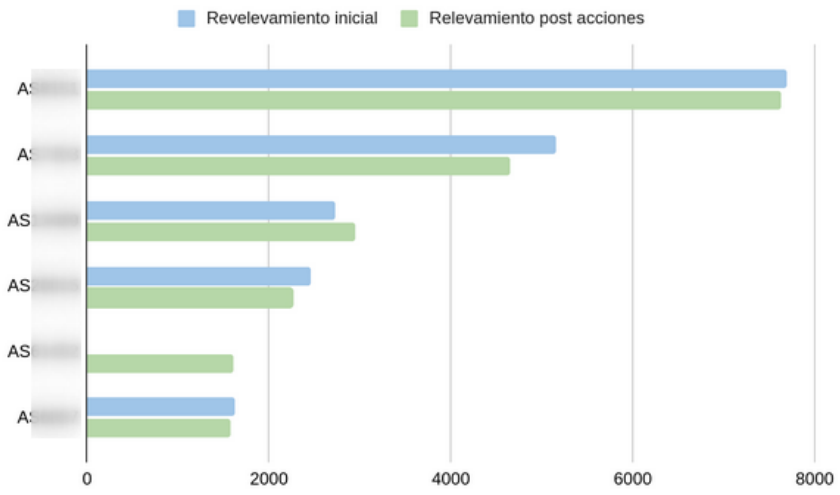



## About the Issues Relating to the Open Resolver Type DNS Protocol

Because servers operating as open resolvers are exposed to the Internet, considerable improvements were observed in terms of DNS related issues for two of the five organizations that were informed about the situation.

Just as in the case of NTPVersion, one organization which had a very low number of open DNS resolvers exposed to the Internet when the initial survey was conducted now appeared among the Top 8.

The following chart reflects the variations experienced by the selected organizations, including the organization observed during the final survey:

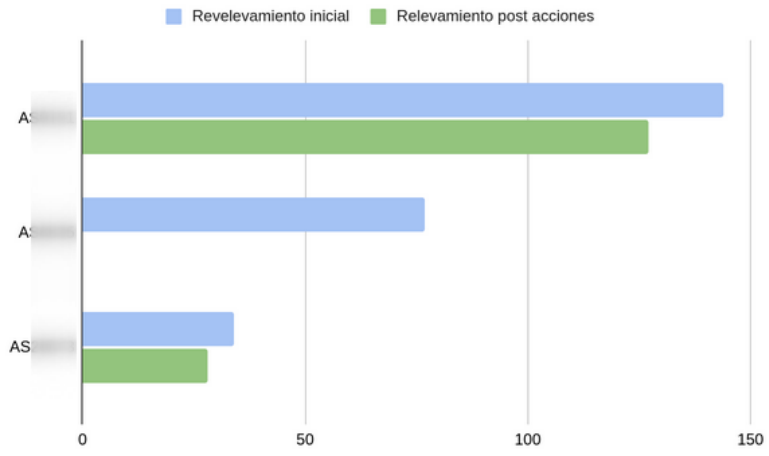



**About the Issues Relating to the CharGen Protocol**

As mentioned earlier, we were able to work in coordination with one LACNIC member to mitigate the issue in 100% of the CharGen services in their ASN exposed to the Internet.

Although the rest of the organizations we contacted did not formally respond to our reports, we noted that he number of exposed CharGen services decreased slightly.

The following chart reflects the variations experienced by the selected organizations.



## *Conclusions*

The study met its objective, as the it allowed mitigating vulnerabilities and therefore improving regional Internet security levels. Likewise, the methodology used by the study promoted interaction between LACNIC CSIRT and its members on security issues, strengthening LACNIC CSIRT's role in sharing tools that allow LACNIC member organizations to provide better services.

The final survey showed organizations with large amounts of vulnerabilities that were not detected in prior surveys. This reflects the fact that actions such as those promoted during this study are always necessary, as additional actors may appear and, with them, new or identical cybersecurity issues.

We propose organizing a webinar to explain these issues, offer support to mitigate related vulnerabilities, and discuss potential actions to increase the level of regional security.

We also recommend that LACNIC CSIRT promote more projects of this type to study security issues across the region. These issues are usually concentrated in a few organizations, so working together contributes to their mitigation.

Finally, we believe it is important to disseminate among the community services such as those provided by Shadowserver. The exposure generated by these sources of information not only helps to raise awareness about the importance of cybersecurity within each organization, but also to consider the need to have a CSIRT to address these issues.

!

***References***


[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/