A Cybersecurity Success Story

LACNIC WARP

Five Years of Computer Security Incident Management

Contents

Executive Summary

Information and communications technologies (ICTs) have become omnipresent in people's daily lives. The benefits they contribute to the welfare of modern societies and economic development are many. However, these technologies are under threat by malicious and ever-changing activities that are continuously on the rise and which can originate anywhere in the world.

This scenario requires coordination frameworks that can cope with the complexity of the interconnection of computer networks and the multiplicity of devices that currently allow people to access cyberspace. The existence of reliable and specialized leaders has become an unquestionable principle in strengthening how people and organizations are positioned when using ICTs.

Within this context, during 2014, LACNIC began to work on the idea of creating a specialized group for the management of security incidents, and this group began operating in March 2015 under the name of LACNIC WARP, the acronym for Warning, Advice and Reporting Point. This decision was taken in line with LACNIC's mission to oversee the correct and secure use of Internet resources in Latin America and the Caribbean and their registration.

It should be mentioned that this is the only RIR that currently provides this type of service to its members. LACNIC offers its members — at no additional cost — incident management services, advice brokering based on an understanding of the needs of its constituency, and the generation of security alerts which it publishes on its website.

It also goes to great lengths to build incident prevention, detection and response capabilities in the region, through its Amparo workshops.

To strengthen trust among entities of a similar nature in the region, LACNIC created and maintains the group of Latin American and Caribbean Computer Security Incident Response Teams (LAC-CSIRT).

At international level, it has signed numerous agreements with recognized international organizations dedicated to fighting computer security incidents and maintains close contact with teams that respond to incidents across the world.

While LACNIC WARP receives any kind of incident report from its community, certain categories are more prevalent than others.

Five years after its creation, LACNIC WARP continues to expand its services and to add value for LACNIC members. It has also achieved regional and international recognition for its contribution to a stable, open, continuously growing and particularly a more secure Internet.

Introduction

The importance that information and communications technologies (ICTs) have gained in people's daily lives over the past three decades is impressive. An almost immediate access to information and knowledge, the immediacy of our contacts, and the timelessness and ubiquity of our access to services are some of the most significant consequences of this transformation.

Forty years ago, if the digital devices that were available at the time had suddenly been shut down, everything would probably have continued to function without major problems. Today, the consequences would be dramatic, as individual and collective well-being and progress are inextricably linked to technological development.

However, excessive confidence in the development of technology and expectations of well-being based on digital devices seem to have increased substantially, far exceeding the capabilities and skills developed to protect ourselves against the misuse of ICTs. It is difficult for States, organizations and individuals to understand the magnitude of the risks involved and, especially, to understand how to address these risks and who to turn to when necessary. In other words, it is not easy to find reliable institutions and specialists in a position to respond to events that can negatively affect information, operations and services.

In a world where threats are increasingly diverse and global, more and more coordination is required to address the complexity of interconnection. Sharing information and being prepared to respond in case of an incident has become an imperative in terms of resource economy, as it helps to strengthen the position of individuals and organizations using ICTs by providing tools in a scenario that does not recognize temporal or geographical boundaries.

In this context, as the Internet Addresses Registry for Latin America and the Caribbean, in 2014 LACNIC began to outline the idea of creating an incident response team, which opened in March 2015 under the name of LACNIC WARP, the acronym for Warning, Advice and Reporting Point. This decision was taken in line with LACNIC's mission to oversee the correct and secure use of Internet number resources in Latin America and the Caribbean and their registration, through initiatives that will provide protection against external factors that might affect them.

This document will describe the history of LACNIC WARP since its inception and its projection into the future. It will also detail the evolution of the various types of abuses that the WARP has managed in a constantly changing, ever-growing and difficult-to-predict threat scenario, and identify its main contributions to the LACNIC member community.

A Brief History of LACNIC WARP

Because of its history and the importance of its activities, since its creation in 2002, LACNIC maintains a close relationship with its members, a community of approximately 10,000 organizations distributed across the different countries of Latin America and the Caribbean. It also has ties with other organizations in the region and around the world, such as the other four Regional Internet Registries (RIRs).

This positioning and closeness with different organizations led LACNIC, in its daily operations, to become aware of information related to potential security incidents that could affect its members. This represented an opportunity and also a challenge: communicating these facts in a timely and accurate manner to help mitigate their effects.

LACNIC WARP was born out of a pressing need to manage the security events reported by LACNIC members, most of them received through an “abuse” mailbox. However, the volume and magnitude of the events that were being reported coupled with the absence of a team specializing in security incident management meant that it was not possible to handle this type of requirements in a timely manner.

In 2014, the idea of creating a group specializing in security incident management began to take shape, a group internationally known as a CERT (Computer Emergency Response Team) or CSIRT (Computer Security Incident Response Team).

LACNIC WARP was created a year later with the mission of coordinating the services needed to strengthen response capabilities in case of incidents related to Internet number resources (IPv4, IPv6), Autonomous System Numbers, and Reverse Resolution in Latin America and the Caribbean. The initiative aimed at contributing to an even greater goal: the constant strengthening of a secure, stable, open and continuously growing Internet, in line with LACNIC's vision.

Its creation and implementation were supported by LACNIC's different departments and managers. Through the Communications department, detailed plans were prepared to disseminate information on this new service among the organization's entire membership base.

The WARP's constituency, i.e., the group of recipients of the services offered by LACNIC WARP, is comprised of LACNIC members and receives incident management assistance at no additional cost. An online incident reporting form and a series of alternative communication channels allow the specialized team to keep up to date with any suspicious activities detected in their computer networks.

However, it should be noted that LACNIC WARP does not have the authority to act on how the community operates their systems. In other words, the decision on how to manage an incident is at the discretion of each affected organization; if required, the WARP adopts an advisory role and offers assistance.

Since its creation, LACNIC WARP publishes security alerts on its website ‹https://warp.lacnic.net/›, as well as contact information, training offerings, and statistics on the incidents that have been managed. It should be mentioned that LACNIC is the only RIR that currently offers this type of services to its members.

Services Offered

Like most CSIRTs, LACNIC WARP offers both proactive and reactive services, which are briefly described below.

Incident Management

Just as other CSIRTs, the main service offered by LACNIC WARP is security incident management. This makes it is an established *point of trust* for reporting suspicious events or sensitive information detected in the networks of the affected organizations.

It also plays a coordination role, as it escalates the incidents that the WARP itself cannot manage to other similar teams. All these activities are carried out under strict levels of confidentiality.

Given the diversity and constant evolution of threats, the volume and variety of incidents treated have been gradually increasing since the early days of the WARP. In addition, the incident process has been perfected in a cycle of continuous improvement.

LACNIC WARP was created in response to the need to deal with reports of security events that affected LACNIC members, and which were mainly received through the *abuse* mailbox. However, the increase in volume, the complexity of the incidents reported, and the lack of a specialized team made it impossible to handle them.

Once the WARP was created, one of its first actions was to study the information received in order to classify it, which also resulted in a compilation of statistics. That's when it was decided to set up a specific email address that would be used for reporting security incidents: info-warp@lacnic.net.

Shortly after, once the website was online, the web form that even today allows reporting security incident was added. Thus, a safe and anonymous brokering environment was provided to facilitate incident identification, characterization, analysis and response, to mitigate the incidents' effects and help restore the affected services.

As customary in this type of activity, all reports received through this form and mailbox undergo a triage assessment to decide whether each incident needs to be managed or, on the contrary, is a simple event that does not require any treatment.

If a security incident that needs to be managed is identified, the incident is classified, a priority is assigned, and a ticket is created with which it will be monitored until it has been closed.

LACNIC WARP receives multiple types of reports from its community, most of which correspond to phishing and malware attacks. The evolution of each of these types of incidents will be explained in further detail in the Statistics section.

Security Alerts and News Bulletins

LACNIC WARP publishes security alerts on its website. The most current or relevant alerts are highlighted under "News" and then compiled in the "Security Alerts" section. The "Articles" section presents documents with information on topics considered relevant to the WARP's constituency. These news items are also distributed to members through periodic newsletters.

Thus, the WARP alerts its community — and in many cases the public in general — so that they will have timely and up-to-date technical information and, if appropriate, can adopt preventive measures.

Based on the incident management reports and the information obtained thanks to the ties with other entities dedicated to the investigation of these issues, statistics are prepared and published monthly, as teams of a similar nature typically do. Later in this document, specific reference will be made to the types of incidents that have been managed.

In addition, taking advantage of the fact that LACNIC has a web portal called MiLACNIC which is used by each member organization to manage its own information, this channel is also used to disseminate information of interest related to cybersecurity issues.

For example, in 2018, a project was implemented to identify Open Resolvers on IPv6 in the region in order to provide members with information on how to properly configure their DNS. This initiative was the result of the numerous reports received by the *abuse* mailbox about this type of issues which, in many cases, were being leveraged to attack other infrastructure components.

This allowed helping potential victims to mitigate security risks affecting the security of their resources. Once the system was automated, this information was integrated into the MiLACNIC platform so that each member would be able to identify and solve potential issues with their resources.

The WARP's plans include continuing to add to this system information regarding other types of alerts that might be affecting our members' resources.

Incorporating additional information on how to improve the configuration of critical services or alerts on the issues that are detected is essential for the development of secure and stable infrastructure, one that is prepared to prevent or detect incidents with high propagation risk in a timely manner.

Training Activities

To promote a culture of cybersecurity and the dissemination of good practices, LACNIC WARP implements an important initiative that involves the creation of incident response capabilities. To do so, the Amparo workshop seeks to train the staff of the organizations that are part of the community served by LACNIC WARP so that they will be able to create their own incident response teams.

These workshops also address good practices related to network security and incident management, such as DNS security and DNSSEC deployment, secure routing through the dissemination of best practices, resource certification and use of RPKI.

The workshops are presented in Spanish and English and include technical, organizational and procedural aspects as well as current topics related to security incident management. These activities are accompanied by presentations that are open to the various sectors that have to do with this discipline, with whom spaces are generated to create awareness among decision makers and specialists, thus contributing to improve how cyber risks are handled.

Resources

The LACNIC team has two highly qualified professionals working full time on incident management, training and research. During 2019, they were assisted by a third person and a multidisciplinary team was formed to address specific tasks to improve their systems.

The team relies on LACNIC's services and resources for anything relating to institutional relations, legal instruments and technological infrastructure. Specialists from other countries of the region may be hired to teach specific topics covered in the Amparo workshops and to develop technical documents. The WARP's entire operating budget is provided by LACNIC.

Community Relations

The WARP's services focus on LACNIC members. To optimize these relations, it generates ties with other organizations of a similar nature, or which have complementary objectives, for example, international organizations such as ICANN, FIRST, the OAS, other RIRs and internationally recognized entities, including Team Cymru, M3AAWG, APWG, and others. It also maintains contact with CERTs/CSIRTs, especially those in Latin America, many of which were created as a result of the Amparo workshops.

At the WARP's initiative, LACNIC has signed cooperation agreements with most of these entities. For example, with Stop, Think & Connect (STC), which implements an important security awareness initiative aimed at the general population and which globally brings together States, regional entities such as LACNIC, non-government organizations and private companies working in the global ICT industry.

Within the framework of the memorandum of understanding signed with FIRST in 2015 and renewed in 2017, several lines of work have been initiated to support the development of cybersecurity incident response capabilities in the region. As part of this agreement, FIRST offers their training programs for LACNIC to deploy with regional teams. Since 2018 and together with Cert.br, Brazil's coordinating CERT, a FIRST symposium is being held annually in Latin America, which includes a plenary conference and several days of training.

LAC-CSIRT

The security-related activities carried out by LACNIC allowed detecting the absence of a space to promote relations among different teams responding to security incidents across the region. As a result, during the LACNIC 21 event held in 2014 in Cancun, Mexico, the creation of the LAC-CSIRT group was proposed, which later helped promote networking among the region's CSIRTs.

The goals of this group include to increase and improve the relations with the members of the regional community, the establishment of a trust network to share information and experiences, and the commitment to work in a coordinated manner on security issues of common interest.

The annual events organized by LACNIC provide these teams with the opportunity to organize face-to-face meetings and the space is consolidating as a space for working and exchanging experiences. This seeks to strengthen each country's capacity to prevent and mitigate the impact of security incidents. LACNIC WARP serves as the group's secretariat.

LACNIC WARP'S DNA: The International Cybersecurity Situation

As the processes and data of individuals and organizations inexorably move into cyberspace, the risks to which they are exposed increase significantly. While some risks are minor and may go unnoticed, others have such a noticeable impact that they strongly affect an entire organization or even an important part of a country's society or economy.

The year 2014 will be remembered for a notable increase in the number of cyberattacks on large companies, mostly based in the United States and Europe, characterized by the breach of the personal and financial data of millions of people. That same year, LACNIC prepared to launch the WARP, adding its current leader to its staff. In October of that year, the initiative was presented in Santiago, Chile, during a FIRST technical colloquium and was very well received by the attendees.

The WARP was launched in March 2015 and a specialized analyst joined the team in the month of October. In addition, the first Amparo workshop was held in San José, Costa Rica and the first memorandum of understanding was signed with FIRST. This recognition by FIRST, a world-class organization that brings together the main CERTs and CSIRTs worldwide, was an early indication of the importance that the WARP would have over the years and of the need for such services in the region.

That same year, a major European mobile phone operator was targeted by an attack that illegally accessed the records of fifteen million customers and two hackers managed to take control of the electronic systems of a moving vehicle, forcing the manufacturer to recall more of a million potentially vulnerable cars.

The following year, the first statistics on the incidents managed in the region were published on the WARP's website and an Amparo workshop was presented in English for the first time in Belize.

In 2016, the world witnessed the theft of more than one million records from a European communications giant and millions of devices were infected with the Mirai malware. This caused a distributed denial of service attack on the infrastructure of one of the world's leading DNS service providers, which ended up affecting an important part of the global Internet.

In May 2017, the world was surprised by the WannaCry ransomware attack, the first attack of its kind on an international scale. Among others, WannaCry directly affected hospital services, telecommunications companies, governments and airports, and indirectly affected organizations of all kinds. That year, LACNIC WARP renewed its agreement with FIRST, signed an agreement with APWG and strengthened its relationship with the M3AAWG.

During 2018, LACNIC WARP launched a project for identifying open resolvers on IPv6, a mechanism that LACNIC members can use to keep their misconfigured servers from accepting recursive queries regardless of their origin and unwittingly becoming part of a denial of service attack. Together with Team CYMRU, it also organized their Regional Internet Security Event in Montevideo, the second of its type to be held in South America.

That year, serious flaws were detected in the privacy mechanisms of major social network companies. As a result, more than 30 million people suffered the consequences of having their personal and contact information exposed. In addition, a ransomware attack disabled the systems of the city of Atlanta, USA, for over a week.

Moreover, banking institutions in Latin America were the victims of theft of their clients' financial data, which caused concern among the governments of those countries.

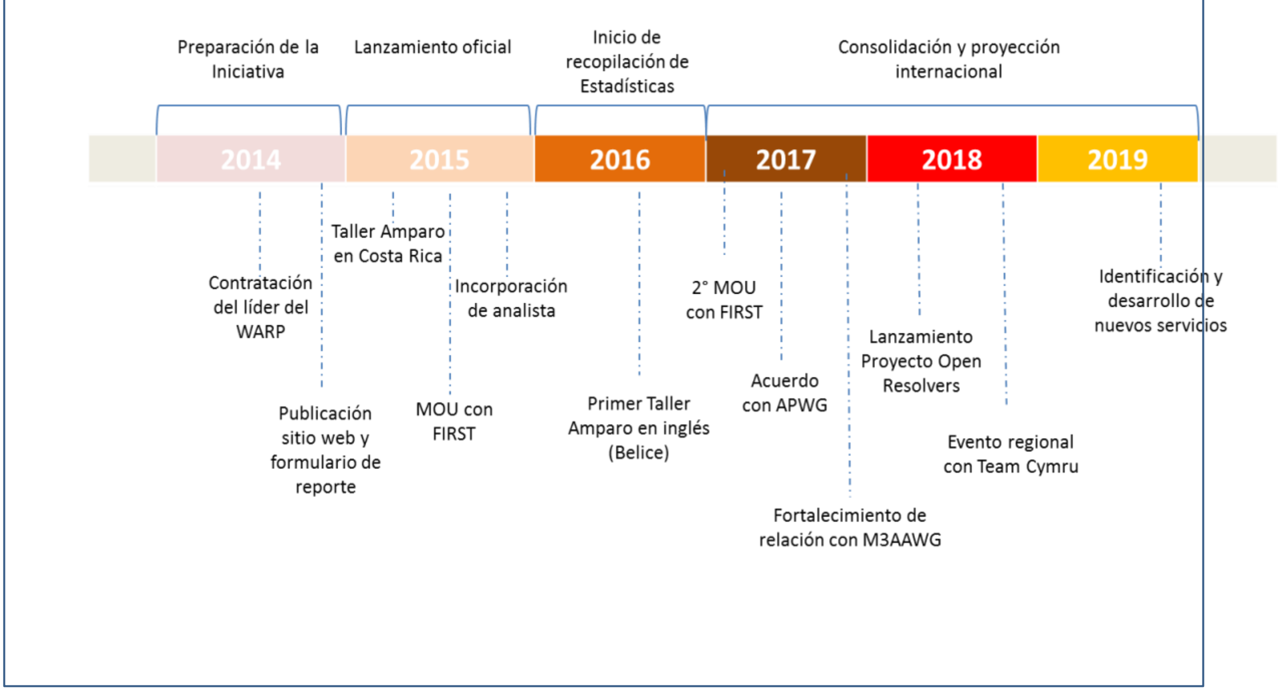
The year 2019 once again saw major personal data leaks and ransomware attacks, and news of cyberattacks perpetrated by global criminal organizations and terrorist groups continue to appear in international media. Some governments have even been accused of originating such attacks.

These attacks target important economic sectors, critical information infrastructure and public agencies. International organizations are starting to discuss the concept of *due diligence* in regard to the measures that the different countries must adopt to avoid the use of the networks and other computer resources located in their territories as a means to attack technological infrastructure in other nations.

In this context, LACNIC WARP is preparing to expand and continues to offer services to the LACNIC member community.

The following image shows the milestones in the history of LACNIC WARP since its creation.

FIGURE 1: MILESTONES IN THE HISTORY OF LACNIC WARP


Preparación de la Iniciativa
Lanzamiento oficial
Inicio de recopilación de Estadísticas
Consolidación y proyección internacional
2014
2015
2016
2017
2018
2019
Taller Amparo en Costa Rica
Contratación del líder del WARP
Incorporación de analista
2° MOU con FIRST
Identificación y desarrollo de nuevos servicios
Lanzamiento Proyecto Open Resolvers
Acuerdo con APWG
Publicación sitio web y formulario de reporte
MOU con FIRST
Primer Taller Amparo en inglés (Belice)
Evento regional con Team Cymru
Fortalecimiento de relación con M3AAWG

Evolution of the Different Types of Incidents

What is known as *incident response* is a process for securing information that was born approximately 30 years ago, when specialists realized that it was necessary to prevent potential disasters within the computer network ecosystem — particularly the Internet — and thus improve the internal objectives involving the protection of information within each organization.

The first security incident response team was created at Carnegie Mellon University in the United States in 1988, after the appearance of the Morris worm, the first self-replicating malware that infected ten percent of the servers connected to ARPANET (the predecessor of what we now know as the Internet).

FIRST was founded a year later in response to the need for specialized teams to share information and cooperate in the management of security incidents. Today, this organization brings together more than 500 teams from across the world and is the largest global trust network in incident response.

Over time and with the increased connectivity between multiple entities, the focus on the expansion of services far exceeded the concerns regarding potential risks. Today, we can see the spectacular variety of services and deployments that technology allows, but also a growing number of incidents which are increasingly reaching the ears of the general public.

In this sense, the infrastructure used to support the services — which is provided by most of the organizations that make up the LACNIC community — becomes a critical link in the value chain of technological development, and the CSIRTs emerge as specialized departments that assist in the prevention of incidents and in their containment and mitigation when they materialize.

Among the services offered by these teams, perhaps the one that affords the greatest benefit to the ecosystem is sharing information on the incidents that occur, a recommendation that is now considered one of the most important good practices in any cybersecurity rulebook.

In order for an organization to be better prepared to protect their information, they must understand the threats they are facing in a scenario where incidents are increasingly common and have a greater impact. An important consideration is that many of these incidents are repeated over the years, for instance, phishing, which we will address later in this document.

In this context, just as the incident response teams that have proliferated worldwide, LACNIC WARP is a predominantly technical entity and its strength clearly lies in recognizing the characteristics of these threats, how they can potentially affect LACNIC members and, most importantly, how they should be managed.

Incidents and the Direct Contribution of LACNIC WARP to the Community

The incidents that can directly affect the community served by the WARP include those that involve the BGP protocol. A BGP hijack is defined as announcing a prefix to another network without the resource holder's consent. This results in the corruption of Internet routing tables.

The WARP classifies this type of security incident as an "unauthorized route announcement." Although they are not very frequent, throughout these years several reports have been received and addressed through the brokering service between parties. Because of their strong impact, this type of incidents represents a major risk. Routing issues can be caused either by deliberate actions or by incorrect configurations. However, in both cases the effects are initially the same.

Typing errors when configuring or updating a system are the most common cause of such incidents. In such cases, when an error is detected and notified, the organizations involved respond almost immediately and correct the problem, thus quickly minimizing its impact. The WARP adds value by receiving the incident report, assessing it, and immediately communicating it to the persons involved so that they can take corrective actions as soon as possible. It acts as a broker between the affected parties.

While there are records of this type of cases since late 1997, in 2017 and based on the analysis of a series of incidents that had already been managed, the WARP's R&D department decided to produce a specific article with a series of general recommendations aimed at preventing incidents that could potentially have extremely serious consequences. These problems are evidenced by connectivity failures, users' complaints regarding issues when trying to access certain websites, and also by other more serious consequences.

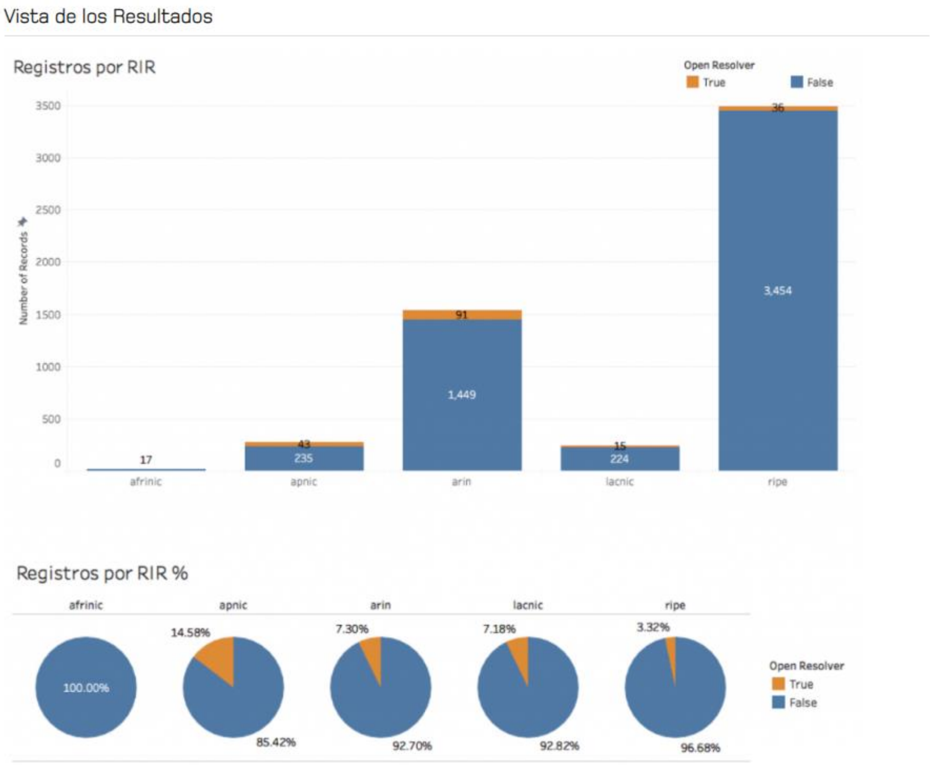
In these cases, it is extremely efficient to have a reliable point of assistance and coordination to share information about the incident — both during its first moments and while the incident is being sorted — and then take the necessary actions to prevent such incidents in the future.

While the BGP protocol has weaknesses and room for improvement, in recent years there have also been reports of incidents that originated in government actions and caused problems beyond their national borders. This is another case where it is also important to know their origin.

Another example of a direct action is the identification of DNS open resolvers. Given the size of the IPv4 address space, this is easy to do in IPv4. In IPv6, however, the scenario is very different. Thus, in early 2018, the WARP launched a project for their identification in this version of the protocol.

The results obtained by this project are shown below.

FIGURE 2: RESULTS OF THE OPEN RESOLVER PROJECT



Source: ‹https://warp.lacnic.net/articulos-tecnicos/identificando-servidores-dns-ipv6-open-resolvers›

The efforts to provide information on the origins of this type of incidents and the recommendations (e.g., through newsletters and/or training activities) on how to strengthen potential weaknesses in the operation of IP addressing schemes are contributions of direct value to the community.

Statistics

Statistics on security incidents prepared by a reliable and independent source provide valuable information that can be used for research purposes, as well as to keep up with current trends and propose measures to improve incident response and contribute to their prevention.

In addition to receiving incident notifications submitted by its constituency, since the beginning of its activities, the WARP has signed agreements with other organizations that are also part of the ecosystem to access information on the abuse of the Internet resources managed by LACNIC in order to be able to assist in incident response and also to generate a solid statistical basis.

In this sense and based on the analysis of these statistics and the most relevant types of incidents that have been detected, it is possible to identify niches that can be used to plan awareness-raising and capacity-building strategies for the region. As mentioned earlier, of all the types of incidents registered by the WARP since 2015, the most frequent are the ones that involve phishing and malware.

The earliest incidents handled by LACNIC WARP include phishing and malicious software generically known as malware, and they have persisted over time, not only in the region but also worldwide (a fact that can be clearly seen in WARP statistics).

This premise is directly related to how quickly threats are spreading and to the fact that the WARP and the community of specialists have recognized that there is no such thing as a secure organization. Therefore, sharing information about threats, types of incidents and their modalities among members of a community having similar characteristics represents a major advantage and is an added value for any organization.

Likewise, phishing was mentioned for the first time in 1996 and became popular in 2003 when it started to become a profitable means to commit fraud. Since then, it has not stopped growing. Malware, the general term that covers any type of code designed to access a device without authorization, hasn't stopped growing either.

An essential component in both these cases is human vulnerability, which social engineering uses to achieve its malicious purposes. Hence the importance of the activities implemented by the WARP to train human resources capable of becoming strong links when information must be protected.

Malware, i.e., the software designed to adapt and mutate and thus overcome the barriers presented by its targets, has many purposes, from industrial espionage to credential theft, from capturing devices to use them in botnets for controlling sensors or any other type of action from which criminal organizations can obtain a benefit. Activities that were once considered cause of minor damages, i.e., activities that affected a single organization or a just few individuals, are currently affecting society as a whole and crossing geographical and temporal borders without major difficulties.

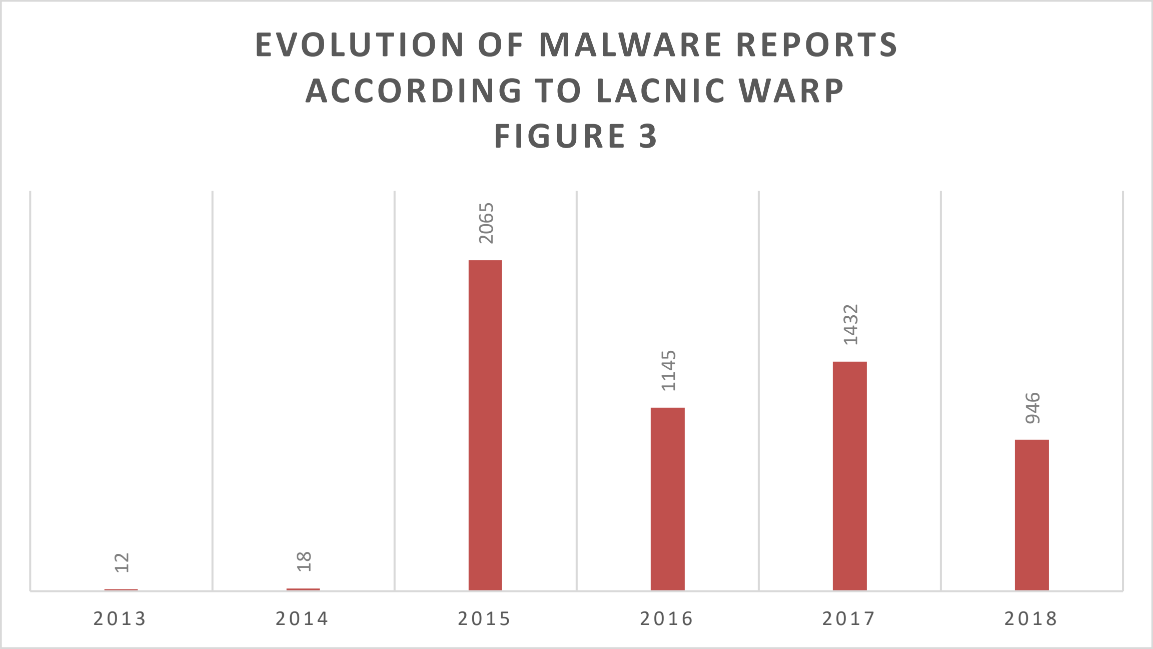
Incidents that used to occur in a segmented or isolated manner now occur in more sophisticated and complex combinations. For example, mass mailing historically sought to distribute ads or announcements. However, for some time now, botnets have been used to distribute malware, either as attachments or through links that lead to websites designed to deceive their users. This has led specialized publications to talk about *malspam* (short for *malware spam* or *malicious spam*).

Likewise, phishing, which in its early days used social engineering techniques to deceive users into revealing their own confidential data such as credit card information or online banking access credentials, continues to be used in the same way but with greater potential, given that digital services are now widespread and extend to many other channels and areas of social life. Examples of this include dating applications, access to medical systems or e-government services, both tax-related and others.

In addition, phishing is currently the preferred method of access for attacks having the greatest impact and the first step in advanced persistent threat (APT) attacks. The latter are planned and executed for prolonged periods of time and they are characterized by their low probability of occurrence and their high impact.

These attacks usually start with a deceptive email which, once it reaches its target, allows access to a device in an unauthorized or illegitimate manner and ultimately steals a large volume of data, generally of a financial nature. In this sense, the incidents observed at the micro level might lead us to think that these are the same attacks, but that they are now typically combined, more complex and have a greater impact.

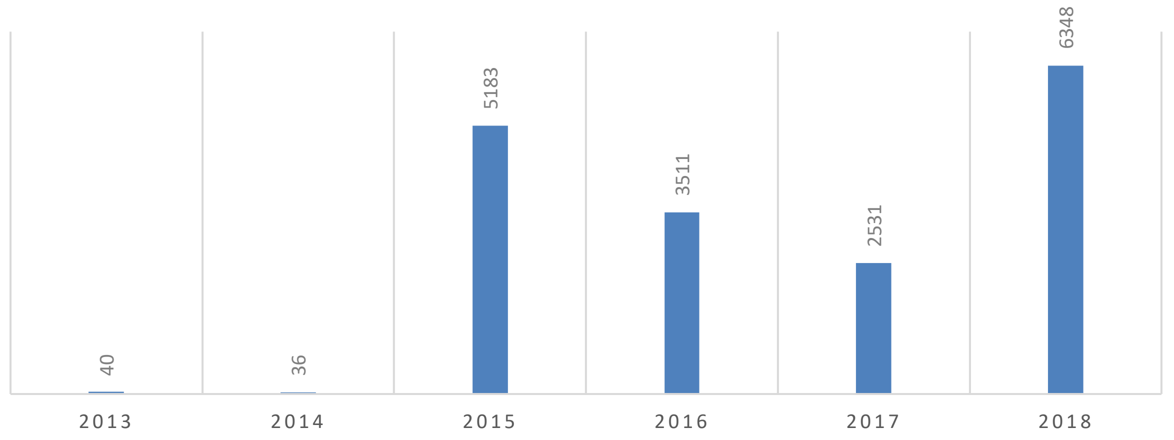
The following charts show the evolution of malware and phishing reports over the years according to LACNIC WARP.



As shown in Figure 3, 2015 was one of the years with the highest incidence of malware in the region. Likewise, in line with global trends, phishing experienced a notable growth in 2018, as shown in Figure 4. Indeed, despite all the initiatives implemented to prevent this type of fraud, far from diminishing, it continues to grow at an alarming rate. As already mentioned, malware is the basis of many attacks on banking systems and has an impact on the countries of the region.

EVOLUTION OF PHISHING REPORTS ACCORDING TO LACNIC WARP

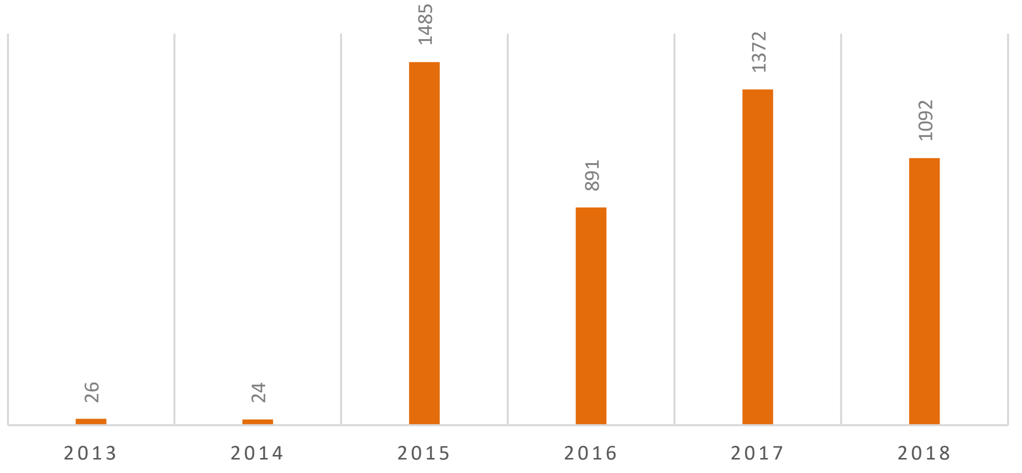
FIGURE 4



The number of covert redirect incidents recorded by LACNIC WARP is also worth mentioning, a form of phishing attack used to redirect victims who believe they are accessing a legitimate Internet address but are actually being redirected to an attacker's website (redirect chains can even be created). This method of attack is typically used to divert IP traffic to a fraudulent site. Combined with other techniques, it can have a serious impact on the public. The following chart shows the evolution of these attacks as recorded by the WARP.

EVOLUTION OF REDIRECT REPORTS ACCORDING TO LACNIC WARP

FIGURE 5



Value Added by the WARP to LACNIC Members

Today, security incidents occur in every layer used for providing the services required by the information society. However, the infrastructure layer is undoubtedly — and in many ways one of the most critical — links. A vulnerability that is quickly detected, reported and fixed results in significant savings both financially and in terms of human resources, and limits potential damages, as essential services can only be provided using fully operational technological infrastructure.

As already mentioned, LACNIC WARP permanently monitors the occurrence and evolution of any security incident that may affect LACNIC members, using this information as input for planning its activities to assist its membership base when responding to an incident as well as to offer awareness and prevention training courses and other activities.

LACNIC WARP also maintains close ties with entities of a similar or complementary nature across the region and worldwide, using the information it collects to help its community prevent, mitigate and eventually quickly and effectively solve the security issues that may affect them.

Having in LACNIC a security alert service, a reliable and specialized source of recommendations and a reporting and brokering point offers a significant advantage to its members who, given their nature and reason for being, carry out activities intrinsically related to technological development in Latin America and the Caribbean.

The excellent relationship with the CSIRTs and CERTs of LAC and other regions allow accessing the latest trends in incident management. By strengthening its trust relationships with these actors, LACNIC WARP increases the effectiveness of its incident management services, as the collaboration of other teams can be requested if necessary or incidents can be escalated in a timely manner.

In this sense, strengthening the security and especially the resilience of technological infrastructure is beneficial for the entire community of organizations to which the WARP provides its services, but also for their clients and users and for the region as a whole. It enables a coordinated response and, eventually, being better prepared to mitigate the effects of an attack.

Conclusions

Much of economic development, the functioning of each State and communications in the Latin American and Caribbean region rely on Internet infrastructure. Therefore, the assignment and administration of number resources, autonomous system numbers and reverse resolution processes are essential for the continued development of the Internet.

In this context, LACNIC WARP and the expansion of the services it has been offering LACNIC members over the past five years have been recognized at regional and international level for the promotion of security incident prevention, detection and response capabilities in the region.

Incidents are reported daily that require a quick and effective response by its team of professionals to minimize their impact. It has been shown that the speed with which action is taken limits the damages and reduces the resources needed to recover the affected services.

One of the critical factors for the WARP's success has been the quality and dedication of its staff, who are clearly committed to the work they carry out. This fully applies to those who work exclusively in incident management, but it also extends to the rest of the technical departments that provide assistance and to the instructors and researchers who permanently support the WARP's activities.

During its first five years of operation, the LACNIC WARP team has managed 600 major computer security incidents in Latin America and the Caribbean. It has also published more than 25 security alerts on events considered to be critical in coordination with other entities devoted to the prevention of cyberattacks.

TORTA Gráfica histórico incidentes gestionados por WARP

In these first five years, LACNIC WARP has organized 19 Amparo workshops across the region for the purpose of strengthening and promoting Computer Security Incident Response Teams (CSIRTs). These workshops have provided training to over 800 regional cybersecurity experts, free of charge.

These efforts have resulted in the creation of incident response teams in Costa Rica, Honduras, Bolivia, Mexico and Ecuador, and the strengthening of existing teams in the other countries visited by LACNIC experts.

Falta: Mapa con los países donde se han realizado Amparos

LACNIC WARP maintains an updated map of the teams that are working on the prevention of cyberattacks in Latin America. This map can be found at ‹https://warp.lacnic.net/mapa-csirts›.

Representatives of these teams have gathered at the ten face-to-face LAC-CSIRT meetings that have been co-located with LACNIC events. These meetings have served to build incident prevention, detection and response capabilities and have strengthened the trust among entities of a similar nature working in the region.

The professional work of the WARP team has allowed it to become part of the global elite of organizations working in computer security. In this sense, LACNIC has signed cooperation agreements with several renowned organizations: FIRST, CERT.br, Message, Mobile, Malware Anti Abuse Working Group (M3AAWG), Anti-Phishing Working Group (SPWG), Stop, Think & Connect (STC) and Team Cymru.

In light of this data, we can say that the initial goals set by the WARP have been met, as it has become a regional leader and gained international recognition.

During these five years, LACNIC WARP has been managed based on LACNIC's mission: to contribute to a stable, open, continuously growing, and especially more secure Internet.

Future Steps

Considering its role in security incident management in Latin America and the Caribbean, one of the main short-term goals of LACNIC WARP is to be accepted as a member of FIRST. To this end, an internal study has been planned that includes applying a maturity model to processes and capacities that allows determining the WARP's current level as well as the level it seeks to achieve, and which will allow implementing the changes needed to correct any issues and reach this goal. Becoming a member of FIRST will provide greater visibility and allow WARP to become part of the largest global security incident management network.

However, the digital transformation that has also affected the organizations in the region presents a growing and changing risk scenario that must be faced and managed. This undoubtedly requires the incorporation of new professionals to further improve the multiple activities the WARP carries out today.

The addition of new automation tools to detect configuration errors, as well as the possibility of making more information available to LACNIC members and the general public to contribute to incident prevention, can be an interesting option worth exploring, particularly if this is to be done in a personalized way, depending on the characteristics of each member.

Along the same line, increasing the security services offered through MiLACNIC can be valuable in contributing to enhance security in the region.

Participating in international security events positions LACNIC WARP as a leader in the field, so it is expected to continue with these activities and to materialize new agreements.

In terms of services to the LANIC WARP constituency, over the next few years they will continue to be customized to the characteristics and needs of each organization that is part of our ecosystem.

Glossary of Terms

APWG: Anti-Phising Working Group.

APT (Advanced Persistent Threat): a type of prolonged and targeted attack through which an intruder gains unauthorized access to a computer network and remains undetected for an extended period with the intention of stealing information or causing damage at the most appropriate time.

Botnet: a number of connected devices that have been captured using malware and that are controlled from a command and control center from where they are sent instructions to execute unauthorized actions. It can affect any type of devices, even IoT devices.

Malware: malicious code generally used to steal data, destroy systems in whole or in part, or hijack information. It can be implanted into a system by means of an email attachment, when downloading an application, and through operating system vulnerabilities.

M3AAWG: Messaging, Malware, Mobile and Anti-abuse Working Group.

Security incident: any event that causes an adverse effect or threatens the availability, integrity and confidentiality of Internet resources, networks and information systems, including violations of established use or security policies.

Pharming (Rogue DNS): exploitation of a vulnerability in DNS server software or users' computers that allows an attacker to redirect IP traffic to a different device.

Phishing: method that attempts to deceive users for the purpose of obtaining sensitive information. Fraudulent resources are presented as legitimate, usually in an attempt to steal a user's access credentials (username, password) and use them to commit fraud. It is typically carried out by fake email messages or when visiting websites of dubious reputation.

Redirect: attack method used to redirect a user from one link to another fraudulent one (redirect chains can also be created). Users are typically redirected to a fraudulent website.

RIR: Regional Internet Registry.

Triage: from the French word *trier*, meaning to sort or prioritize. The stage of incident management that includes the reception of reports, their verification, initial classification and subsequent assignment of each case for their resolution.

Unauthorized prefix advertising or BGP hijacking*:* unauthorized announcement of network prefixes; announcement of routes by unauthorized origins. Route hijacking occurs when a prefix is announced on the Internet by an unauthorized party. This may be either intentional or caused by operational errors.

Acronyms and Abbreviations

APWG	Anti-Phishing Working Group
APT	Advanced Persistent Threat
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
ENISA	European Network and Information Security Agency
FIRST	Forum of Incident Response Teams
IOT	Internet of Things
M3AAWG	Messaging, Malware and Mobile Anti-Abuse Working Group
OAS	Organization of American States
RIR	Regional Internet Registry
RPKI	Resource Public Key Infraestructure
ICT	Information and Communications Technology
WARP	Warning, Advice and Response Point

List of Figures