LACNIC's WARP

Guillermo Cicileo

lacnic

www.lacnic.net

About LACNIC

LACNIC – RIR – Internet Registry for LAC region

- Non gov organization
- Set up in Uruguay in 2002
- We are responsible for the assignment and managemente of the Internet resources:
  - IPv4, IPv6
  - Autonomous System Numbers
  - Reverse DNS
- Area service: 33 territories

Introduction

Graciela Martínez - Head of WARP

WARP stands for:

- Warning
- Advice &
- Reporting Point

Constituency:

- LACNIC´s members

Coordinating role:

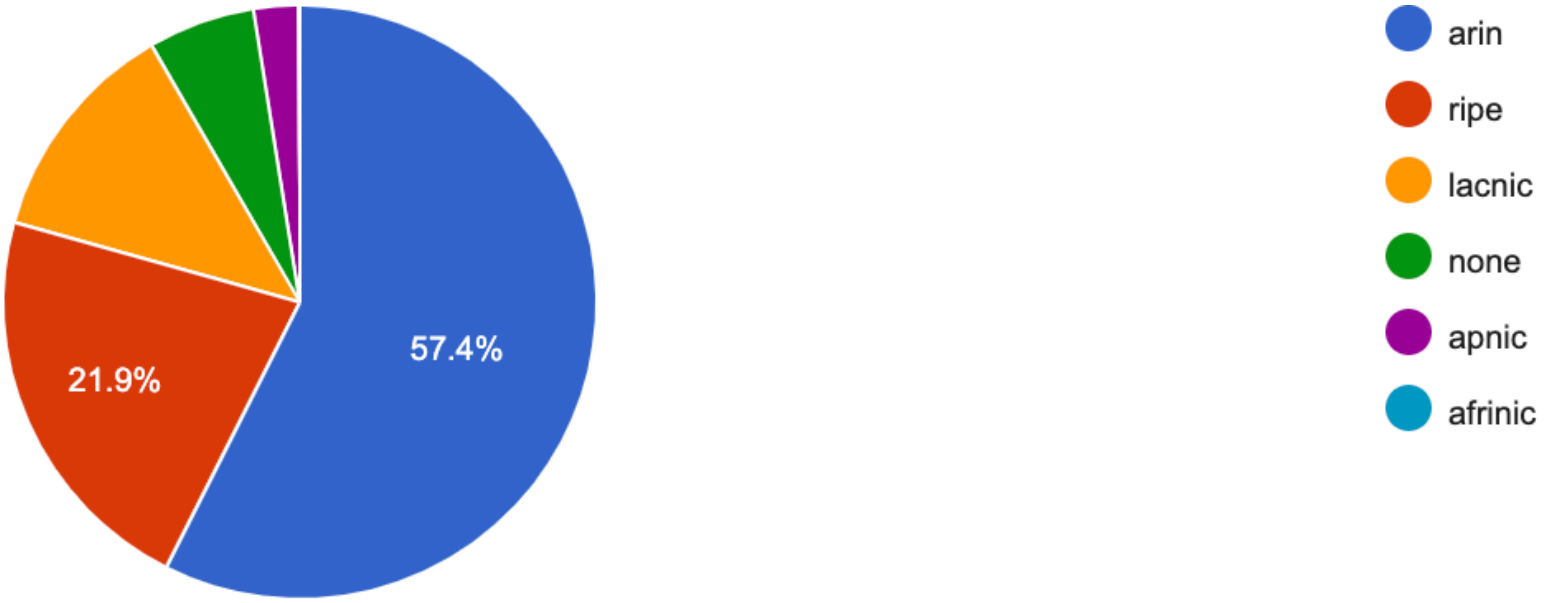
- LACNIC WARP does not have the authority to act on the operations of its community's systems

Types of incidents reported to WARP from other organizations

https://warp.lacnic.net/en/estadisticas

lacnic

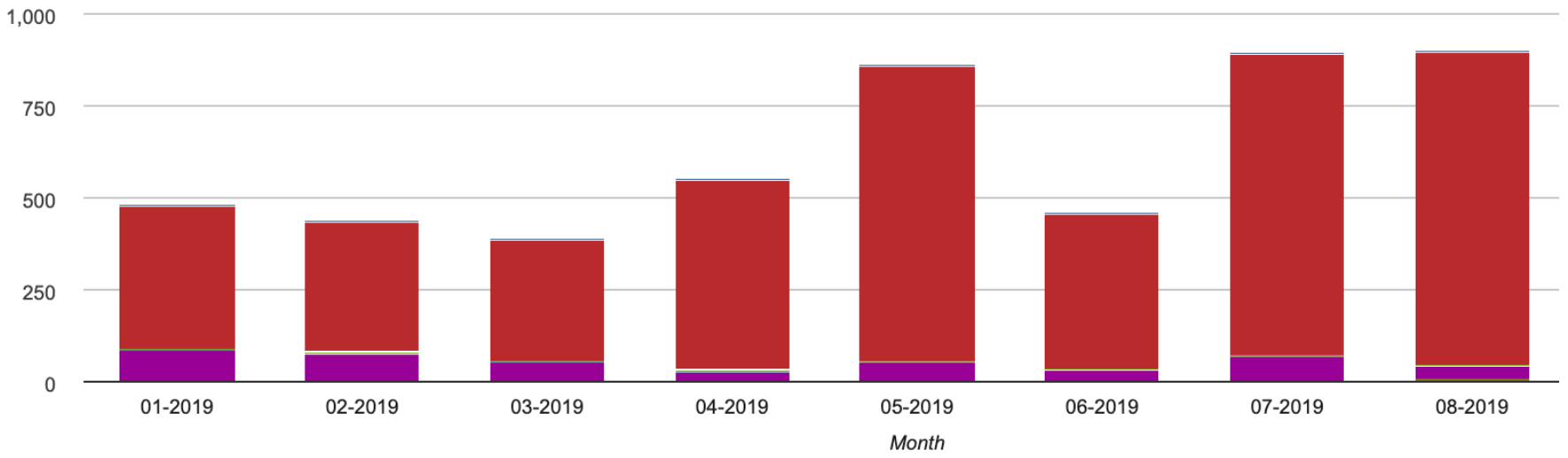
Types of incidents reported to WARP group by regions



https://warp.lacnic.net/en/estadisticas

lacnic

Phishings reported to WARP from other organizations 2019



https://warp.lacnic.net/en/estadisticas

lacnic

Types of incidents managed by WARP

This chart shows the historical percentage of each type of incident managed by WARP

https://warp.lacnic.net/estadisticas#Warp_Tipos_de_Incidentes

lacnic

Most common Botnets affecting resources in our region

https://warp.lacnic.net/estadisticas#Tipos_de_Botnet_Regional

lacnic

Phishing & Botnets

- We have been targeted by spear phishing and the CEO fraud
  - Staff awareness
- Some problems when managing a phishing report:
  - GDPR – whois – no contact available
- Botnets
  - Systems out-of-date

Honeynet

Our needs:

- First-hand knowledge of the most frequent types of security attacks in Latin America and the Caribbean
- Help our consituency: Warning Reports and Recommendations

- Network of honeypots that allow us to view security incidents in real time and learn the modus operandi of the most common attacks in the region
  - Telnet & SSH
  - Designed to log all the activities of the attackers

- Comprised of a series of sensors distributed throughout different organizations with which we seek to establish relationships of trust.

Active sensors:
AR, CW, DR, EC (3), MX, UY (2)

How to participate ?

- Project site: https://warp.lacnic.net/honeynet/

- email
  - dario@lacnic.net
  - gmartinez@lacnic.net

Open Resolvers IPv6

- Open Resolver - DNS resolver that allows queries from everywhere

- They are a threat on the Internet
  - For instance:
    - Amplification attacks - A small query can return a huge response
    - They are susceptible to cache poisoning

- WARP and Abuse – we receive lots of reports about Open Resolvers that belong to our region that were/are attacking other systems

Open Resolvers IPv6

- We decided to use our own information:
  - Reverse DNS Server under our management
  - Reverse Root Server -“D” : d.ip6-servers.arpa
  - Only receives queries from other DNS resolvers

- We use the IP list to do a query for a specific domain and check the answer
  - Query refused or time-out ? → OK
  - Get an answer? → not OK → Warning with recommendations to fix the misconfiguration, server hardening and DNSSEC implementation

- https://warp.lacnic.net/dns-open-resolvers-con-ipv6

BGP Hijacking

- Unauthorized prefix advertisement - An ASN announces a route without having the right to do it
- For example by announcing a more specific route
- Hijacking or Unauthorized prefix advertisement ?
- It is very difficult to prove the “bad” intention of it!
  → Warning! (email)

RPKI – LACNIC

LACNIC operates the Resource Certification System (RPKI) for the number resources assigned in the region

RPKI is a public key infrastructure which offers providers additional tools to verify a client's right to use Internet resources.

A Route Origination Authorization (ROA) is a digitally signed object that explicitly authorizes a specific AS to originate a group of addresses

In order to generate certificates and ROAs, LACNIC's RPKI system can be accessed at: http://milacnic.lacnic.net

https://www.lacnic.net/1018/2/lacnic/resource-certification-system-rpki

Where can I report a security Incident in LAC region?

- LACNIC´s CSIRT - WARP

https://warp.lacnic.net/reportar-incidente/

CSIRTS in America Latina and the Caribbean

lacnic

What we do to fight cybercrime?

- Warnings to our constituency when the Internet resources are used for bad purposes
- MOU´s – information sharing
- Trainings – Amparo (more than 15)
  - Aprox 1000 tech & prof
- Security conferences together with our main events
  - FIRST Colloquim
  - FIRST Symposium
  - RISE – Team Cymru
- LAC-CSIRTs – face-to-face meetings
- We encourage working in a multistakeholder approach

Thank you !

For more information contact Graciela Martínez
gmartinez@lacnic.net

lacnic

www.lacnic.net