Latin America and Caribbean Anti-Abuse Working Group **LAC-AAWG**

Lighting Talks – LACNOG-LACNIC
22 de setembro de 2017
Montevideo, UY

Lucimara Desiderá

LACNIC, the Latin America and Caribbean Network Information Center, and M3AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group, have the support of a new partner: LACNOG, the Latin America and Caribbean Network Operators Group.

On February 8th 2017, LACNOG ratified the charter for the Latin America and Caribbean Anti-Abuse Working Group. LAC-AAWG combines knowledge and expertise from LACNIC, LACNOG, and M3AAWG to develop a self-sustaining anti-abuse community in the LAC region.

LAC-AAWG will serve as a convening forum for network operators and anti-abuse experts. LAC-AAWG's mission is to foster dialog among existing communities and working groups, fomenting the development of anti-abuse recommendations and best current operational practices (BCOPs) that address region-specific and global issues. LAC-AAWG will also act as the voice of the LAC region in the global anti-abuse community, further cementing the exchange of anti-abuse ideas, knowledge, and best practices between the LAC region and M3AAWG's global community.

LAC-AAWG will also coordinate regional anti-abuse awareness activities like presentations and tutorials targeting Latin America and Caribbean relevant communities. These engagements aim to educate the LAC operator community on, and foster adoption of, regional and global anti-abuse best practices and operations.

The founding co-chairs of LAC-AAWG are Christian O'Flaherty from ISOC and Lucimara Desiderá from CERT.br/NIC.br. The first face-to-face LAC-AAWG community meetings will take place during LACNIC 27, in Foz do Iguaçu, Brazil, on May 22-26, 2017. In partnership with M3AAWG, these activities will comprise presentations, BOFs, and tutorials on anti-abuse best practices.

www.lacnic.net/en/web/anuncios/2017-amenazas-en-linea-se-fortalece

2 CA-1990-02: Internet Intruder Warning

Original issue date: March 19, 1990
Last revised: September 17, 1997
Attached copyright statement

A complet

There hav
entitled "C
ferred to a

At this poi
not have h
tempts on systems using known security vulnerabilities. All of these vulnerabilities have been previously reported. Some national news agencies have referred to a "virus" on the Internet; the information we have now indicates that this is NOT true. What we have seen and can confirm is an intrude

It is possit
tempts hav

2. Exploit accounts without passwords or known passwords (accounts with vendor supplied default passwords are favorites).

   Also uses finger to get account names and then tries simple passwords.

   Scan your password file for extra UID 0 accounts, accounts with no password, or new entries in the password file. Always change vendor supplied default passwords when you install new system software.

VMS SYSTEM ATTACKS:

13. The intruder exploits system default passwords that have not been changed since installation.

    Make sure to change all default passwords when the software is installed. The intruder also guesses simple user passwords. See point 1 above for suggestions on choosing good passwords.

BCOPs under development

- Suggestions for new BCOPs development
  - **Security Requirements for CPE Acquisitions ???**
  - **Security Requirements for CPE Management???**

How to contribute

- Engage in the development of best practices / BCOPs
  - contribute to BCOPs content
  - being the editor/reviewer of BCOP

Thank you!

Questions?
Volunteers ?!!?

lucimara@cert.br
oflaherty@isoc.org

Where to subscribe

- List **BCOP** bcop@lacnog.org
  - open list of the BCOP Working Group (LACNOG) for discussion of Best Current Operational Practices;
- List **LACNOG** lacnog@lacnog.org
  - open mailing list for discussion of general topics on network operations, not limited to Security;
- List **LAC-SEC** seguridad@lacnic.net
  - open mailing list for discussion of general topics on Information Security, not limited to incident handling.
- List **LAC-CSIRTs** lac-csirts@lacnic.net
  - A closed mailing list for discussion of topics related to incident handling. Institutional membership is required. Restricted to CSIRTs members.