

# M<sup>3</sup>AAWG @ LACNIC Update: Developing an Anti-Abuse Community

Jesse Sowell, PhD

Special Advisor to M<sup>3</sup>AAWG

Cybersecurity Fellow at Stanford Center for International Security  
and Cooperation

27 September 2016

LACNIC 26, San Jose, Costa Rica



# LACNIC-M<sup>3</sup>AAWG Partnership

## Why Are We Here?



---

## Comunicado de prensa

### Para publicación inmediata

## LACNIC y la comunidad latinoamericana de seguridad operacional se unen a M<sup>3</sup>AAWG para combatir las amenazas en línea

*San Francisco, 31 de marzo de 2016* – LACNIC, el Registro Regional de Internet para América Latina y el Caribe, se ha unido al Grupo de Trabajo Antiabuso de Mensajes, Malware y Móvil para colaborar en temas globales de ciberseguridad. LACNIC es también el foro que convoca al Grupo de Operadores de Red de LAC; LACSEC, el Foro de Seguridad de Redes de la región; y LAC-CSIRT, un foro regional de respuesta a incidentes de seguridad. Como parte de una asociación mutua para luchar contra las amenazas en línea, M<sup>3</sup>AAWG también se ha unido a LACNIC para interactuar con estos proveedores de servicios y comunidades de seguridad en línea.

[Esta interacción continua](#) permitirá que el M<sup>3</sup>AAWG tenga acceso a expertos regionales en tendencias operacionales y antiabuso y les dará la oportunidad de desarrollar soluciones conjuntas relevantes que aborden las tendencias actuales en el área de la ciberseguridad y la ciberdelincuencia. LACNIC, el Registro de Direcciones de Internet para América Latina y el Caribe, tendrá acceso a la variada experiencia de los miembros del M<sup>3</sup>AAWG y su permanente trabajo en el desarrollo de mejores prácticas.

# LACNIC-M<sup>3</sup>AAWG Partnership

## Why Are We Here?



Esta interacción continua permitirá que el M<sup>3</sup>AAWG tenga acceso a expertos regionales en tendencias operacionales y antiabuso y les dará la oportunidad de desarrollar soluciones conjuntas relevantes que aborden las tendencias actuales en el área de la ciberseguridad y la ciberdelincuencia.

de Seguridad de Redes de la región; y LAC-C<sup>3</sup>SIRT, un foro regional de respuesta a incidentes de seguridad. Como parte de una asociación mutua para luchar contra las amenazas en línea, M<sup>3</sup>AAWG también se ha unido a LACNIC para interactuar con estos proveedores de servicios y comunidades de seguridad en línea.

Esta interacción continua permitirá que el M<sup>3</sup>AAWG tenga acceso a expertos regionales en tendencias operacionales y antiabuso y les dará la oportunidad de desarrollar soluciones conjuntas relevantes que aborden las tendencias actuales en el área de la ciberseguridad y la ciberdelincuencia. LACNIC, el Registro de Direcciones de Internet para América Latina y el Caribe, tendrá acceso a la variada experiencia de los miembros del M<sup>3</sup>AAWG y su permanente trabajo en el desarrollo de mejores prácticas.

# Developing a LAC Anti-Abuse Community Presentations This Week



| Title  | Presenters  | Time                                   | Location   |
|--|---|--|------------|
| M <sup>3</sup> AAWG Best Common Practices                          | Dennis Dayman, M3AAWG Board and Vice-Chair  | 1800-1900<br>Tuesday<br>27 September   | Greco      |
| Economics of Abuse Operations: Concepts and Application to Hosting | Tobias Knecht, CEO Abusix<br>Jesse Sowell, M <sup>3</sup> AAWG, Stanford<br>Matthew Stith, M <sup>3</sup> AAWG, Rackspace | 1630-1800<br>Wednesday<br>28 September | Aguamarina |

# Developing a LAC Anti-Abuse Community Presentations This Week



| Title  | Presenters  | Time                                   | Location   |
|--|---|--|------------|
| M <sup>3</sup> AAWG Best Common Practices                          | Dennis Dayman, M3AAWG Board and Vice-Chair  | 1800-1900<br>Tuesday<br>27 September   | Greco      |
| Economics of Abuse Operations: Concepts and Application to Hosting | Tobias Knecht, CEO Abusix<br>Jesse Sowell, M <sup>3</sup> AAWG, Stanford<br>Matthew Stith, M <sup>3</sup> AAWG, Rackspace | 1630-1800<br>Wednesday<br>28 September | Aguamarina |

# Overview

- What abuse and anti-abuse?
- What is M<sup>3</sup>AAWG?
- What is M<sup>3</sup>AAWG's role in anti-abuse?
- How to contribute!



# Anti-Abuse Dynamics



# Anti-Abuse and Attribution

## The Blame Game

Unraveling precisely why a network is on a blocking list is not always easy

**What are the pragmatics of anti-abuse and attribution?**

- What constitutes abuse?
- How have abuse indicators evolved?
- Fundamental economics of abuse and anti-abuse operations





# Anti-Abuse and Attribution

## Prescriptive Ethos

“all information exchanges on the Internet *should be consensual*, and unless you choose to receive [traffic] from a third party, you should not *have to accept it*”<sup>1</sup>

Just because there is a *legitimate route* to a destination doesn't mean all traffic *using that route* is legitimate

Provides a ***prescriptive ethos***, but doesn't help with ***practical application***



<sup>1</sup> Adapted from an early definition by MAPS <sup>9</sup>

# Anti-Abuse and Attribution Evolution, Issues, and Pragmatics

“abuse is what customers complain about”<sup>2</sup>

1. Subjective → Objective indicators
2. Indicators are *always* error-prone
3. Continuous development and evaluation of indicator performance
4. Focus has shifted from inbound to outbound (attribution)
5. Who bears the burden?
6. Economics of indicators and anti-abuse operations



<sup>2</sup> Definition offered by Dave Crocker

# M<sup>3</sup>AAWG Overview

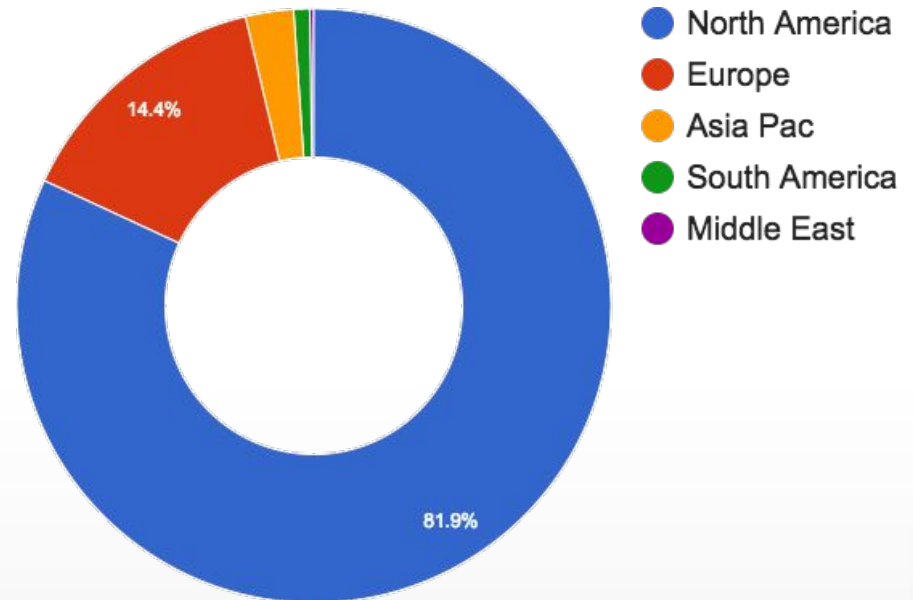
# Who is M<sup>3</sup>AAWG?

## Industry Anti-Abuse Organization



“The Messaging, Malware and Mobile Anti-Abuse Working Group (M<sup>3</sup>AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation”

- 200 member orgs worldwide
- 300-400 conference participants
- technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - Supporting technologies
  - Industry collaboration
  - Informing Public Policy



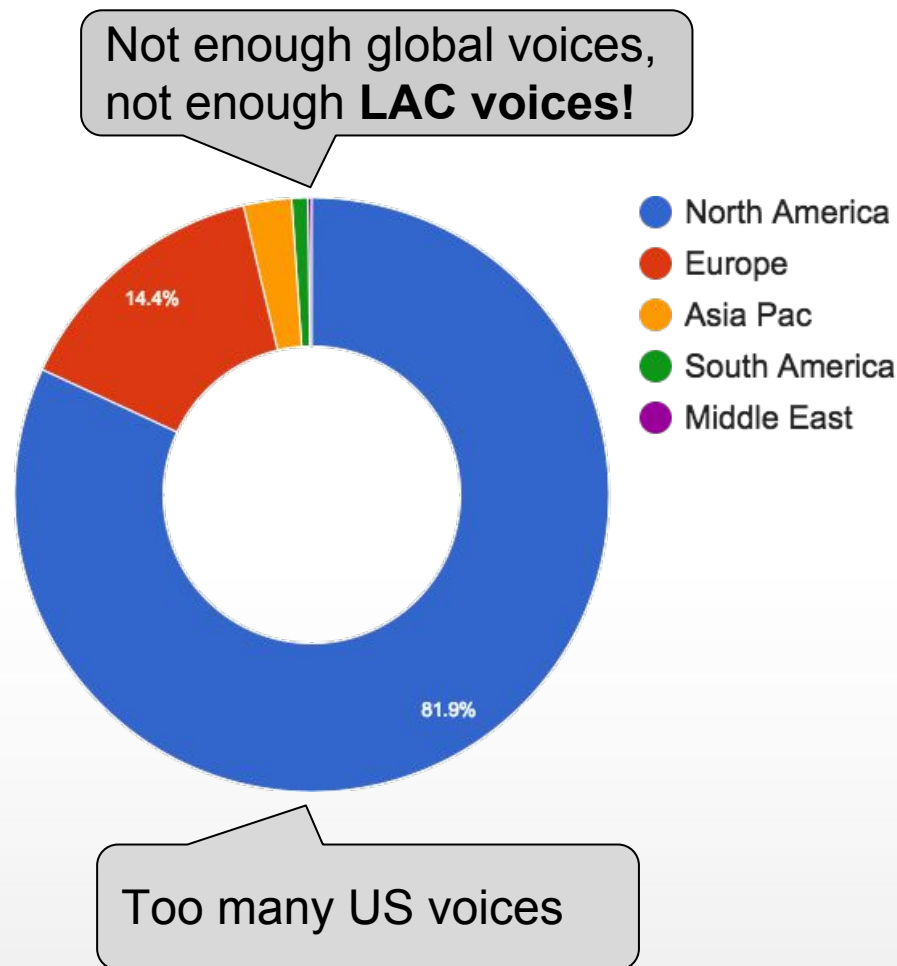
# Who is M<sup>3</sup>AAWG?

## We Need LAC Contributions



“The Messaging, Malware and Mobile Anti-Abuse Working Group (M<sup>3</sup>AAWG) is where the industry comes together to work against botnets, malware, spam, viruses, DoS attacks and other online exploitation”

- 200 member orgs worldwide
- 300-400 conference participants
- technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - Supporting technologies
  - Industry collaboration
  - Informing Public Policy



# What Does M<sup>3</sup>AAWG Do?

## Distill Industry Knowledge into BCPs



### The “M” cubed:

- **Messaging:** abuse on any messaging platform, from e-mail to SMS texting
- **Malware:** abuse is often just a symptom and vector for viruses and malicious code
- **Mobile:** addressing messaging and malware issues emerging on mobile as an increasingly ubiquitous platform

### Develop and Publish:

- Best practice papers
- Position statements
- Training and educational videos

### Public Policy and Industry Guidelines

<https://www.m3aawg.org/for-the-industry/published-comments>

### The Anti-Bot Code of Conduct for Internet Service Providers

<https://www.m3aawg.org/abcs-for-ISP-code>



# What Does M<sup>3</sup>AAWG Do?

## Distill Industry Knowledge into BCPs

### Latest BCPs

- [M<sup>3</sup>AAWG Best Current Practices For Building and Operating a Spamtrap, Ver. 1.2.0](#)
- [Using Generic Top Level Domain Registration Information \(WHOIS Data\) in Anti-Abuse Operations](#)
- [M<sup>3</sup>AAWG Introduction to Traffic Analysis](#)

### Ongoing Work

- DDoS Protection for All
- DDoS Victim Preparation Guide

**M<sup>3</sup>AAWG**  
MESSAGING MALWARE MOBILE

Messaging, Malware and Mobile Anti-Abuse Working Group

**M<sup>3</sup>AAWG Best Current Practices  
For Building and Operating a Spamtrap**  
Version 1.2.0  
Updated August 2016

Table of Contents

INTRODUCTION .....  
SPAMTRAP GOALS/PURPOSES .....  
SPAMTRAP ADDRESSES .....  
ISSUES WITH ADDRESSES .....  
IMPLEMENTATION CONSIDERATIONS .....  
ANALYSIS .....  
SECURITY .....  
INFORMATION SHARING .....  
HINTS AND PITFALLS .....  
CONCLUSION .....  
REFERENCES .....

**M<sup>3</sup>AAWG**  
MESSAGING MALWARE MOBILE  
ANTI-ABUSE WORKING GROUP

Messaging, Malware and Mobile Anti-Abuse Working Group

**M<sup>3</sup>AAWG Introduction to Traffic Analysis**  
June 2016

**Introduction**

Protecting against pervasive monitoring and the use of encryption continues to be a major focus for the messaging industry. M<sup>3</sup>AAWG has already published initial recommendations for deploying TLS,<sup>1</sup> mitigating Man-in-the-Middle attacks<sup>2</sup>, and using forward secrecy to secure data<sup>3</sup> to help the messaging community understand how to better secure email in transit. Now M<sup>3</sup>AAWG would like to bring awareness to a different type of risk – a form of attack called *traffic analysis*. In this paper, we outline the key characteristics of traffic analysis, discuss potential ways to avoid it, and consider the advantages and disadvantages of deploying preventative measures.

**Understanding Traffic Analysis with Respect to Messaging and Network Traffic**

The content of messages encrypted with PGP/GPG (GNU Privacy Guard)<sup>4</sup> or S/MIME<sup>5</sup> is generally highly resistant to eavesdropping. Even if a third party manages to get a copy of a PGP/GPG-encrypted email (or an S/MIME-encrypted email), they are not likely to be able to decrypt and read it. However, even messages that are perfectly protected with end-to-end encryption remain potentially subject to traffic analysis attacks.

To understand the difference, consider the following summary table of email message elements visible to an intermediary SMTP server utilizing TLS for transmitting messages and their availability for traffic analysis purposes:

| Email message elements  | Vulnerable to traffic analysis? |
|---|---------------------------------|
| Return-Path: header   | Yes                             |
| Received: headers   | Yes                             |
| From: header  | Yes                             |
| To: header  | Yes                             |
| CC: header  | Yes                             |
| Date: header  | Yes                             |
| Subject: header   | Yes                             |
| Message-ID: header  | Yes                             |
| Any/all other headers   | Yes                             |
| Size of the message   | Yes                             |
| Time message was received                                       | Yes                             |
| Apparent encryption used by message                             | Yes                             |
| Message contents (assumed to be possibly or actually encrypted) | No                              |

In a traffic analysis attack, the focus is not on the content, but on the message headers and other externally-observable artifacts associated with the message or the communication process itself. The summary table

**M<sup>3</sup>AAWG**  
Messaging, Malware and Mobile Anti-Abuse Working Group  
P.O. Box 28920 • San Francisco, CA 94128-0920 • [www.m3aawg.org](http://www.m3aawg.org)



# What Does M<sup>3</sup>AAWG Do?

## Who Do We Work With?



- Unsolicited Commercial Enforcement Net
  - Operation Safety Net
- Internet Society
  - Provided training material
- i<sup>2</sup>Coalition
  - Hosting BCP
- EastWest Institute
  - 2013 Cyber Security Award for China & India Work
- Anti-Phishing Working Group (APWG)
  - Anti-Phishing Best Practices for ISPs and Mailbox Providers
- **LACNIC!**
  - **Looking forward to updating BCPs to reflect dynamics in the LAC region**



# Anti-Abuse Community Development

# Developing and Anti-Abuse Community Fostering Collaboration

**M<sup>3</sup>AAWG's** work relies on:

- ***working group participation***, in the spirit of
- ***cooperation***, to create
- effective and efficient ***anti-abuse outcomes***
- in a ***trusted*** environment



# Chatham House Rules

## Community Trust and Safety

**Trust is key to all of M<sup>3</sup>AAWG's activities**

- **Respect M<sup>3</sup>AAWG anonymity:** Blogging, tweeting, posting, and publishing content from M<sup>3</sup>AAWG requires permission from *presenters and M<sup>3</sup>AAWG*
- **Outcome:** M<sup>3</sup>AAWG participants can *safely* share information critical to solving technical abuse problems without fear of retribution from other industry actors or criminals whose illegitimate businesses impacted by anti-abuse efforts



# Chatham House Rules

## Ongoing Reminder



### What occurs in a M<sup>3</sup>AAWG meeting cannot be shared outside the membership

- **New!** Attendees can blog, tweet and post about **selected, pre-approved sessions only**. **These sessions open with a GREEN LIGHT slide. No posting or external communications from all sessions with a RED LIGHT slide when the session is closed.** Please reference @maawg or #m3aawg37 where we are also tweeting.
- In all cases, respect M<sup>3</sup>AAWG anonymity: No publishing people or company names, except as cited on the official M<sup>3</sup>AAWG channels: @maawg, facebook.com/maawg, google plus
- No use of Wireshark or similar products on the M<sup>3</sup>AAWG network
- No photography - No video - No audio recording
- Any exception requires written permission from the Executive Director and may require permission from the session members
- All meeting attendees must wear and have their M<sup>3</sup>AAWG badge visible at all times during the meeting
- Please silence all electronic devices; be courteous to those listening to the presentations
- DO NOT LEAVE YOUR BELONGINGS UNATTENDED. Be aware and cautious at all times

**Treat all attendees respectfully in and out of sessions. No less will be tolerated.**

**Please review our meeting Conduct Policy at <http://www.m3aawg.org/page/m3aawg-conduct-policy>**

For questions, please contact Jerry Upton at: [jerry.upton@m3aawg.org](mailto:jerry.upton@m3aawg.org)

# Committees, SIGs, and BoFs

## Where the Work is Done

### Technical

Messaging  
Malware  
Mobile  
DDoS SIG  
Internet of Things BoF

### Collaboration Committee

Abuse Desk SIG  
Anti-Phishing SIG

### Public Policy Committee

Information Sharing SIG  
Bot & Messaging Metrics

Senders Committee

Hosting Committee

Pervasive Monitoring SIG

Identity Management SIG

Voice & Telephony Abuse SIG

Brands SIG





# Contributing to Working Groups

## Participation and Commitments

|                       | Low   | Medium  | High   |
|-----------------------|---|---|--|
| <b>Time</b>           | Quick but necessary tasks   | Tasks like annotating a document or finding a speaker                                     | Document champion or editor, chairs and vice chairs, board   |
| <b>Expertise</b>      | Basic anti-abuse knowledge---a willingness to put forth effort and learn! | Experience or with workflows of quick and medium tasks; specialized expertise in a domain | Experience at multiple meetings and in multiple medium leadership roles  |
| <b>Accountability</b> | Ability to turn around short tasks quickly                                | Ability to organize low tasks and update collaborators on status of medium tasks          | Take responsibility for major M <sup>3</sup> AAWG initiatives such as a full session, meeting planning, reports like the Botnet report |



**[www.m3aawg.org](http://www.m3aawg.org)**

**Questions?  
Volunteers?!?!?**

**Drop me a line at  
[jsowell@m3aawg.org](mailto:jsowell@m3aawg.org)**