M^{3}AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

What is M^{3}AAWG

Jesse Sowell, PhD
4 May 2016
LACNIC 25, La Habana, Cuba

Who Am I?

Jesse Sowell, PhD in Technology, Management and Policy

(January 2015, MIT)

M^{3}AAWG Affiliations:

Vice Chair of Growth and Development Committee

Special Advisor to the Chairman

NANOG Affiliation:

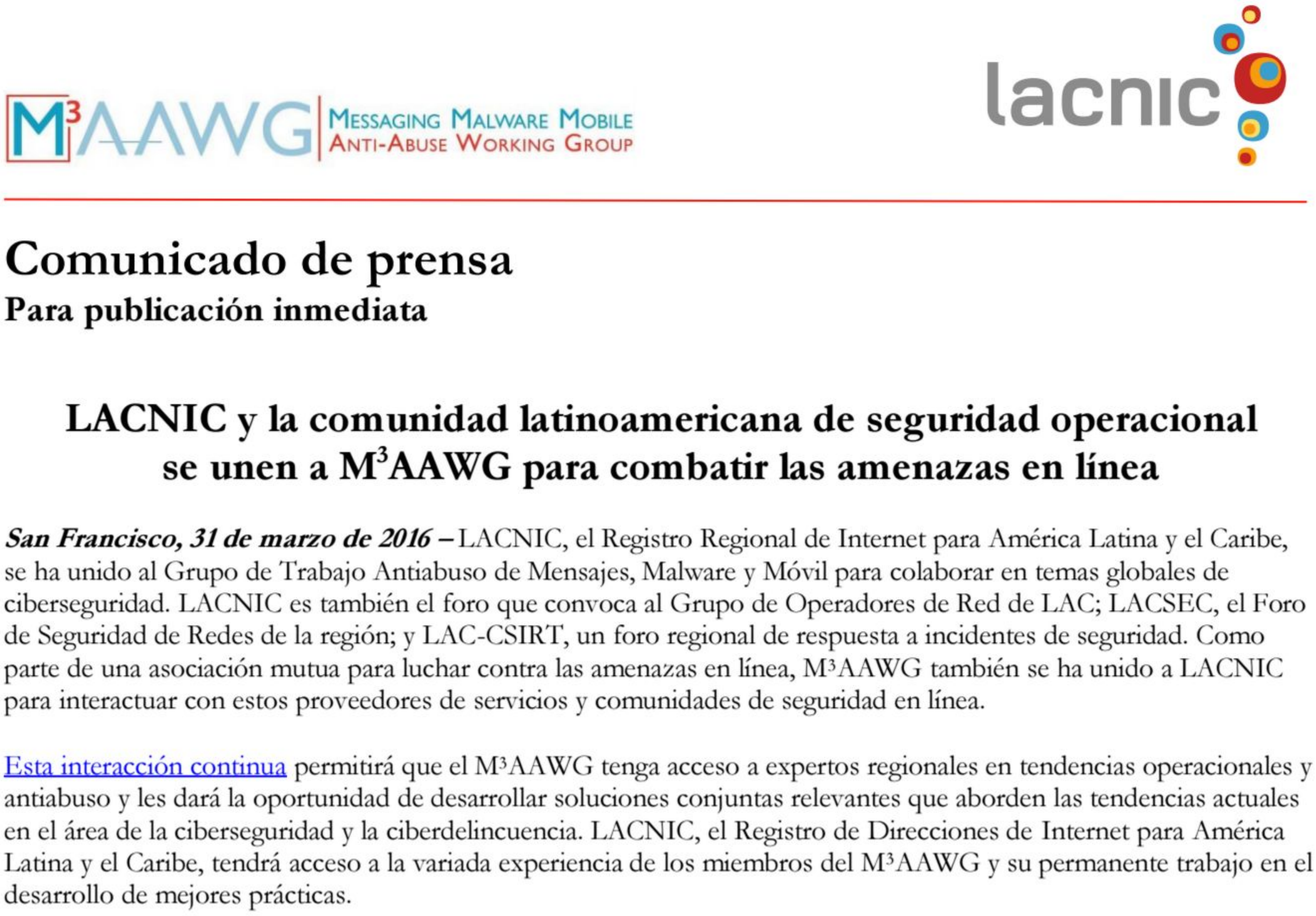
NANOG Program Committee Member

Research Affiliations:

Stanford University Center for International Security and Cooperation

(starting October 2016)

LACNIC-M^{3}AAWG Partnership
Why am I Here?



M^{3}AAWG | MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP

lacnic

Comunicado de prensa
Para publicación inmediata

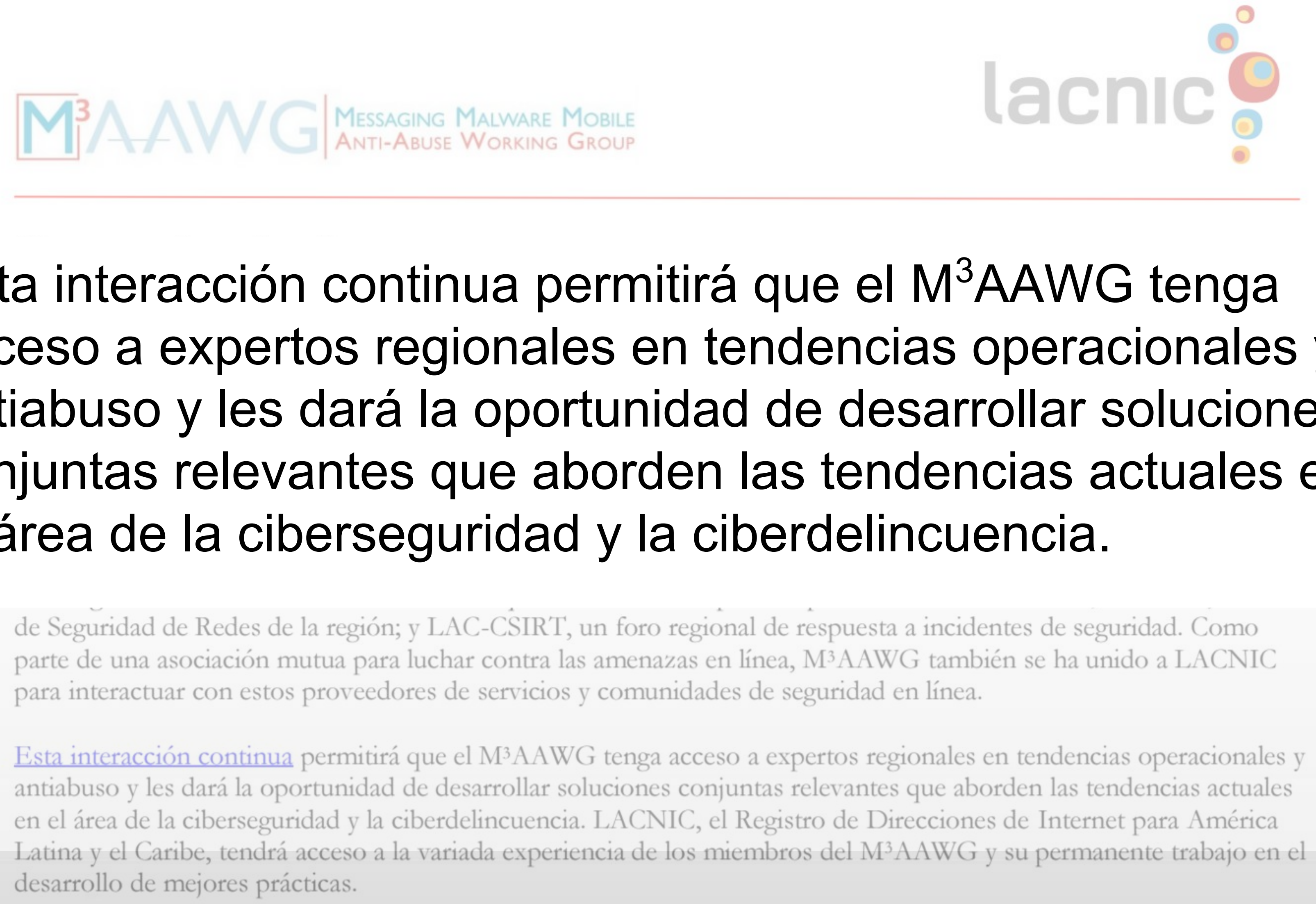
LACNIC y la comunidad latinoamericana de seguridad operacional se unen a M^{3}AAWG para combatir las amenazas en línea

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^{3}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^{3}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^{3}AAWG y su permanente trabajo en el desarrollo de mejores prácticas.

LACNIC-M^3AAWG Partnership
Why am I Here?

Esta interacción continua permitirá que el M^3AAWG 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.



M^3AAWG Messaging Malware Mobile Anti-Abuse Working Group
lacnic

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^3AAWG 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^3AAWG 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^3AAWG y su permanente trabajo en el desarrollo de mejores prácticas.

Overview

- ➔ What is the anti-abuse community?
- ➔ What is M^{3}AAWG?
- ➔ What is M^{3}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" [1]

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***

[1] Adapted from an early definition by MAPS

Anti-Abuse and Attribution Evolution, Issues, and Pragmatics

"abuse is what customers complain about"[2]

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

[2] Definition offered by Dave Crocker

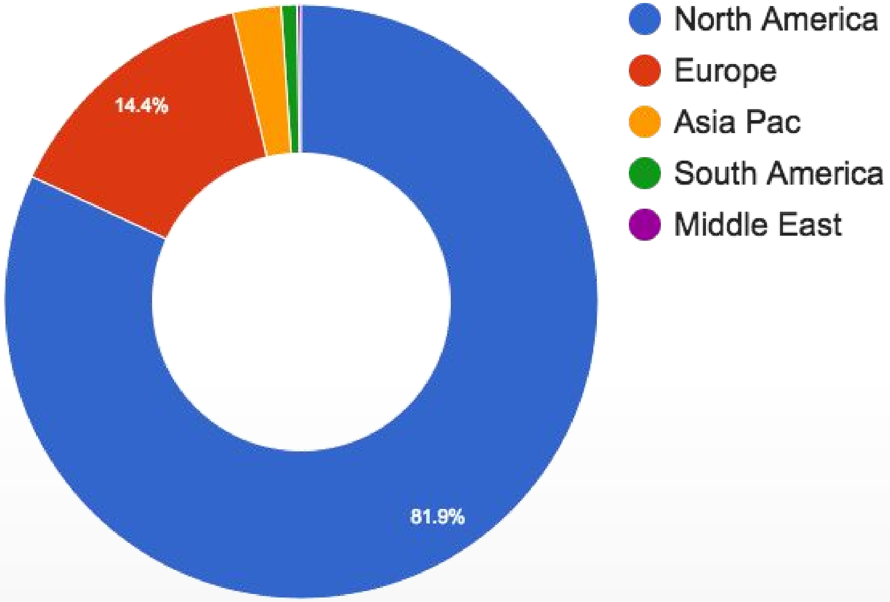
M^{3}AAWG Overview

Who is M³AAWG?
Industry Anti-Abuse Organization

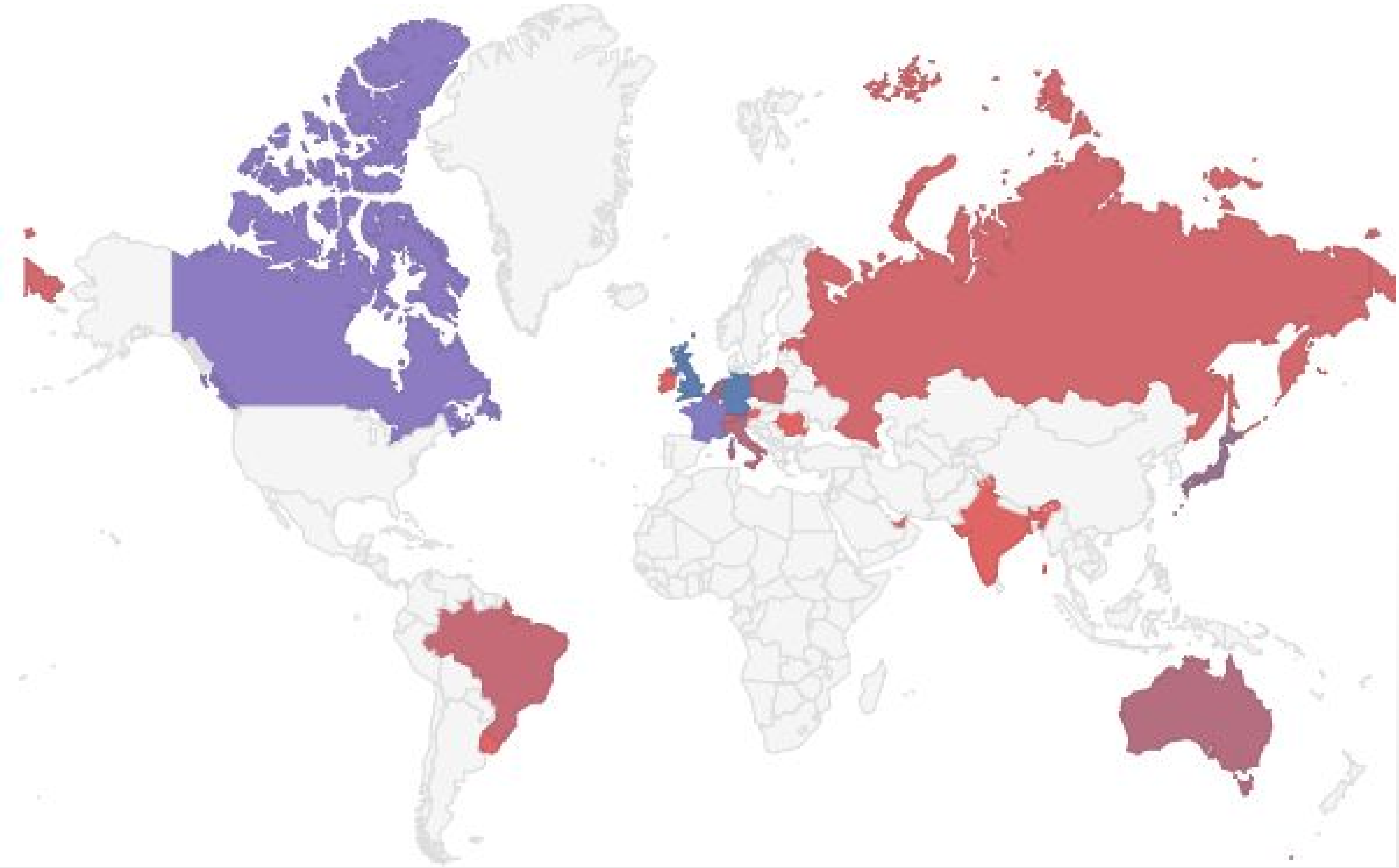
M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

"The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) 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^{3}AAWG?
San Francisco CA Meeting Attendance



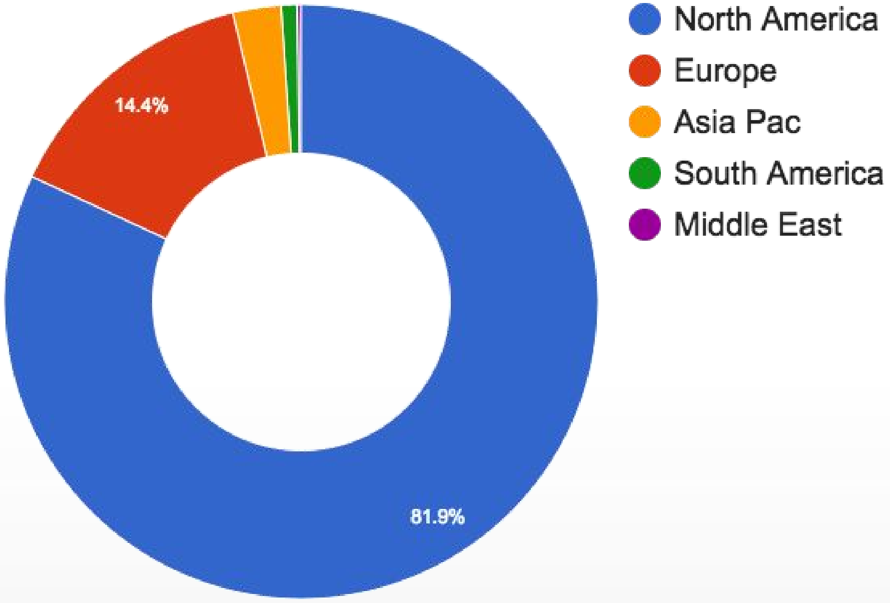
Who is M3AAWG?
We Need Your Contributions

M3AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

"The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) 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

Not enough global voices, not enough **LAC voices!**



Too many US voices

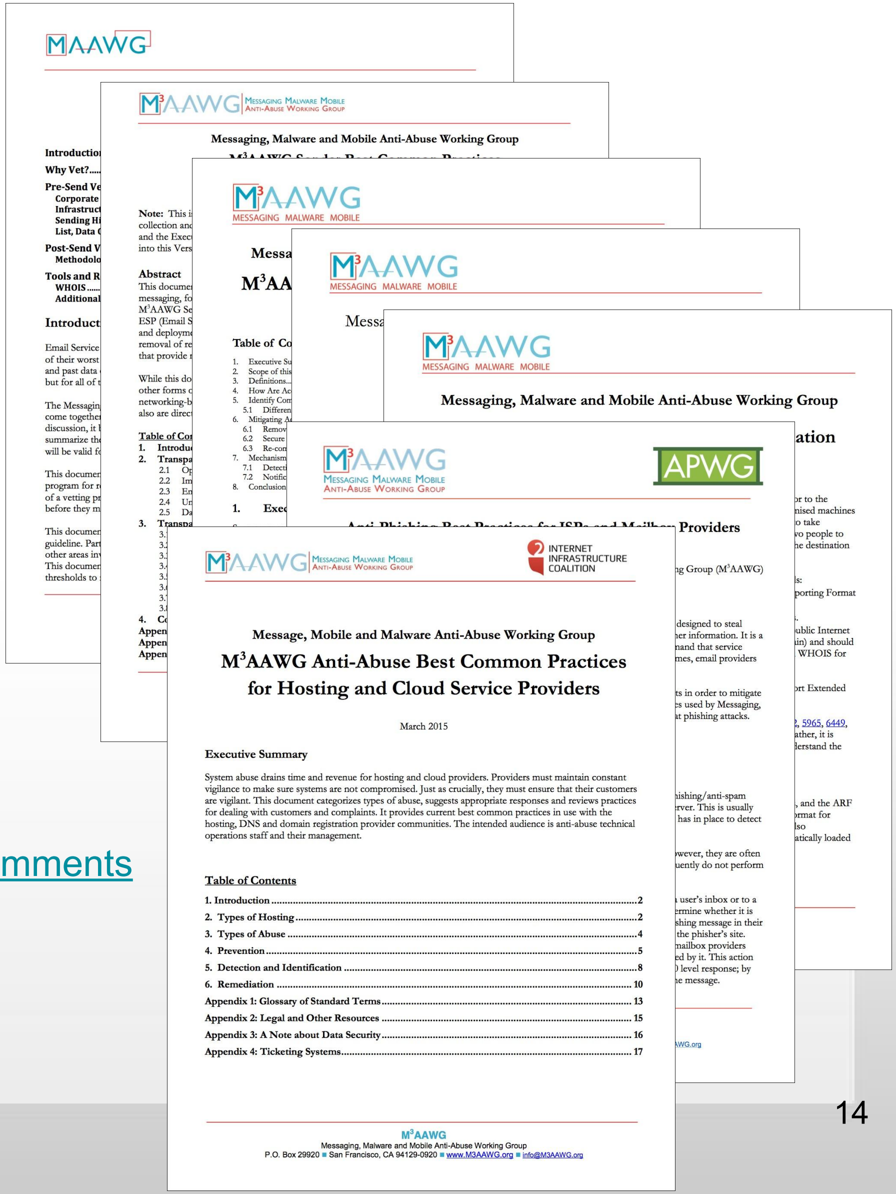
What Does M3AAWG Do?
Distill Industry Knowledge into BCPs

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



Message, Mobile and Malware Anti-Abuse Working Group

M3AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers

March 2015

Executive Summary

System abuse drains time and revenue for hosting and cloud providers. Providers must maintain constant vigilance to make sure systems are not compromised. Just as crucially, they must ensure that their customers are vigilant. This document categorizes types of abuse, suggests appropriate responses and reviews practices for dealing with customers and complaints. It provides current best common practices in use with the hosting, DNS and domain registration provider communities. The intended audience is anti-abuse technical operations staff and their management.

Table of Contents

M3AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
P.O. Box 29920 ■ San Francisco, CA 94129-0920 ■ www.M3AAWG.org ■ info@M3AAWG.org

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

Who Do We Work With?

- ➔ London Action Plan
  - – Operation Safety Net
- ➔ Internet Society
  - – Provided training material
- ➔ i^2Coalition
  - – 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

Fostering Collaboration

M^{3}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^{3}AAWG's activities

- ➔ **Respect M^{3}AAWG anonymity:** Blogging, tweeting, posting, and publishing content from M^{3}AAWG requires permission from *presenters and M^{3}AAWG*
- ➔ **Outcome:** M^{3}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^{3}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^{3}AAWG anonymity: No publishing people or company names, except as cited on the official M^{3}AAWG channels: @maawg, facebook.com/maawg, google plus
- No use of Wireshark or similar products on the M^{3}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^{3}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

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

Participation and Commitments

	Low	Medium	High
Time	Quick but necessary tasks	Tasks like annotating a document or finding a speaker	Document champion or editor, chairs and vice chairs, board
Expertise	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
Accountability	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^{3}AAWG initiatives such as a full session, meeting planning, reports like the Botnet report

www.m3aawg.org

Questions?
Volunteers?!!?