M³AAWG @ APNIC Cooperation SIG: Anti-Abuse Community Development

Jesse Sowell, PhD

Special Advisor to M³AAWG; Vice-Chair of Growth and Develop Directing Outreach
NANOG Program Committee
Cybersecurity Fellow at Stanford Center for International Security and Cooperation

APNIC 44
Taichung, Taiwan
12 September 2017

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Introduction

Anti-Abuse and Attribution
Prescriptive Ethos

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

"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
Prescriptive Ethos

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

“abuse is what customers complain about”[2]

“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
[2] Definition offered by Dave Crocker

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

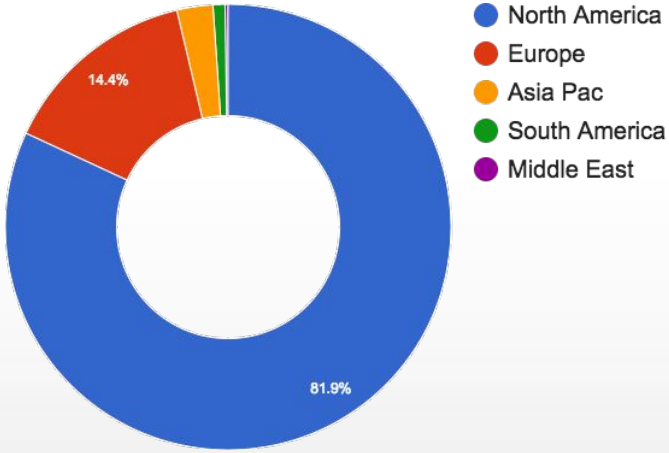
M3AAWG and Anti-Abuse Overview

Who is M³AAWG?
Constituencies and Demographics

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"

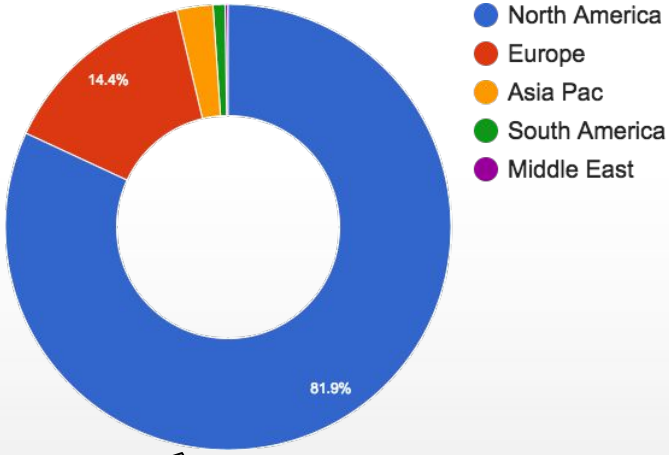
- ➔ 200 member orgs "worldwide"
- ➔ 300-400 conference participants
- ➔ technology-neutral, *non-political* working body focusing on operational issues of Internet abuse
  - Supporting technologies
  - Industry collaboration
  - Informing Public Policy



Who is M³AAWG?
We Need AP Contributions

"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



Too many US voices

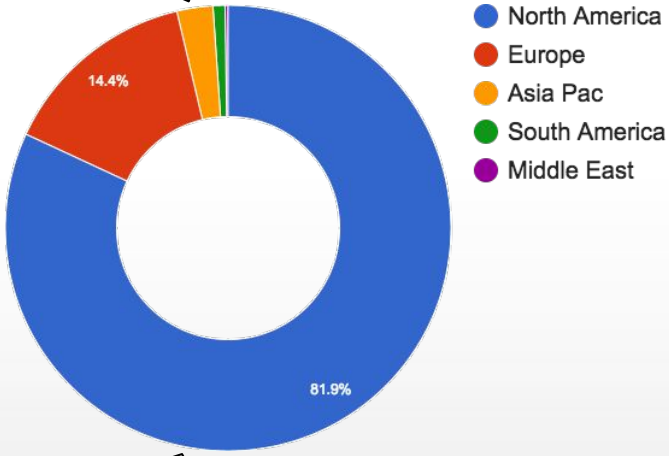
Who is M³AAWG?
We Need AP Contributions

"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

M³AAWG
Messaging Malware Mobile Anti-Abuse Working Group

Not enough global voices, not enough **AP 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:

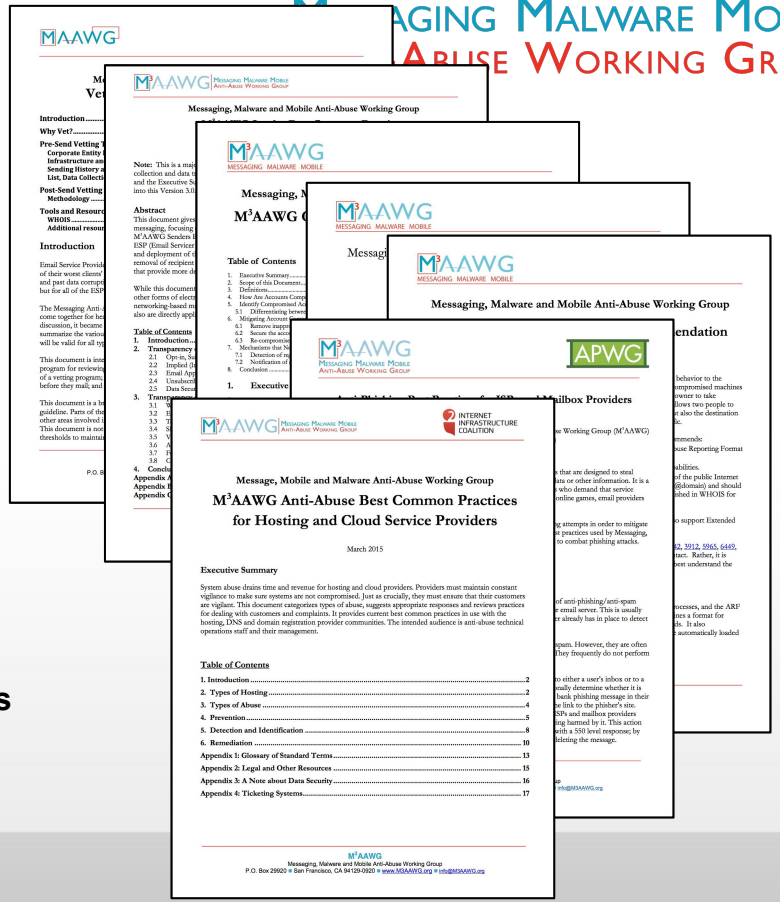
- ➔ Best practice papers
- ➔ Position statements
- ➔ Training and educational videos

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



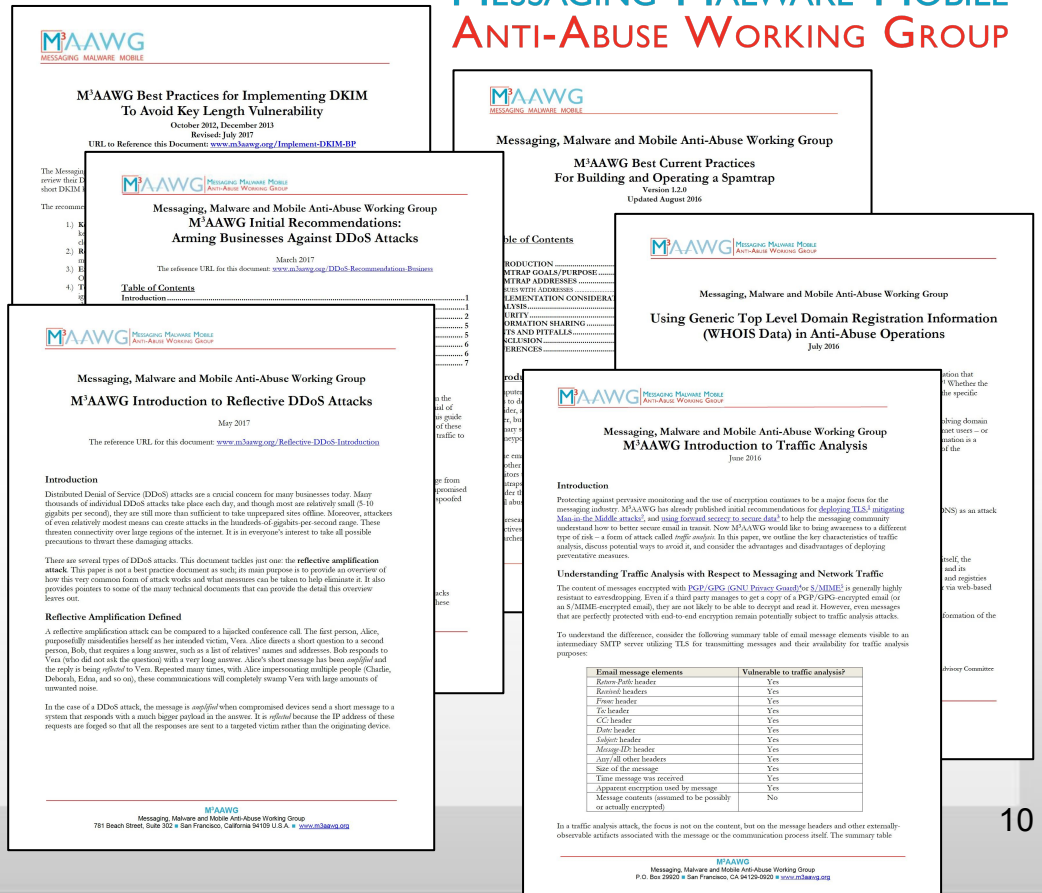
What Does M³AAWG Do?

Distill Industry Knowledge into BCPs

Latest BCPs

- ➔ M³AAWG Best Practices for Implementing DKIM to Avoid Key Length Vulnerability
- ➔ M³AAWG Best Practices Introduction to Reflective DDOS Attacks
- ➔ M³AAWG Initial Best Practices: Arming Businesses Against DDOS Attacks
- ➔ M³AAWG 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
- ➔ M³AAWG Introduction to Traffic Analysis

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group



What Does M³AAWG Do?

Who Do We Work With?

Unsolicited Commercial Enforcement Net

➔ Operation Safety Net

Internet Society

➔ Provided training material

i²Coalition

➔ 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

LAC-AAWG

➔ **Updating and developing BCPs to reflect LAC dynamics**

AF-AAWG

➔ **In progress with AfricaCERT**

What Does M³AAWG Do?

Who Do We Work With?

Unsolicited Commercial Enforcement Net

➔ Operation Safety Net

Internet Society

➔ Provided training material

i²Coalition

➔ 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

LAC-AAWG

➔ **Updating and developing BCPs to reflect LAC dynamics**

AF-AAWG

➔ **In progress with AfricaCERT**

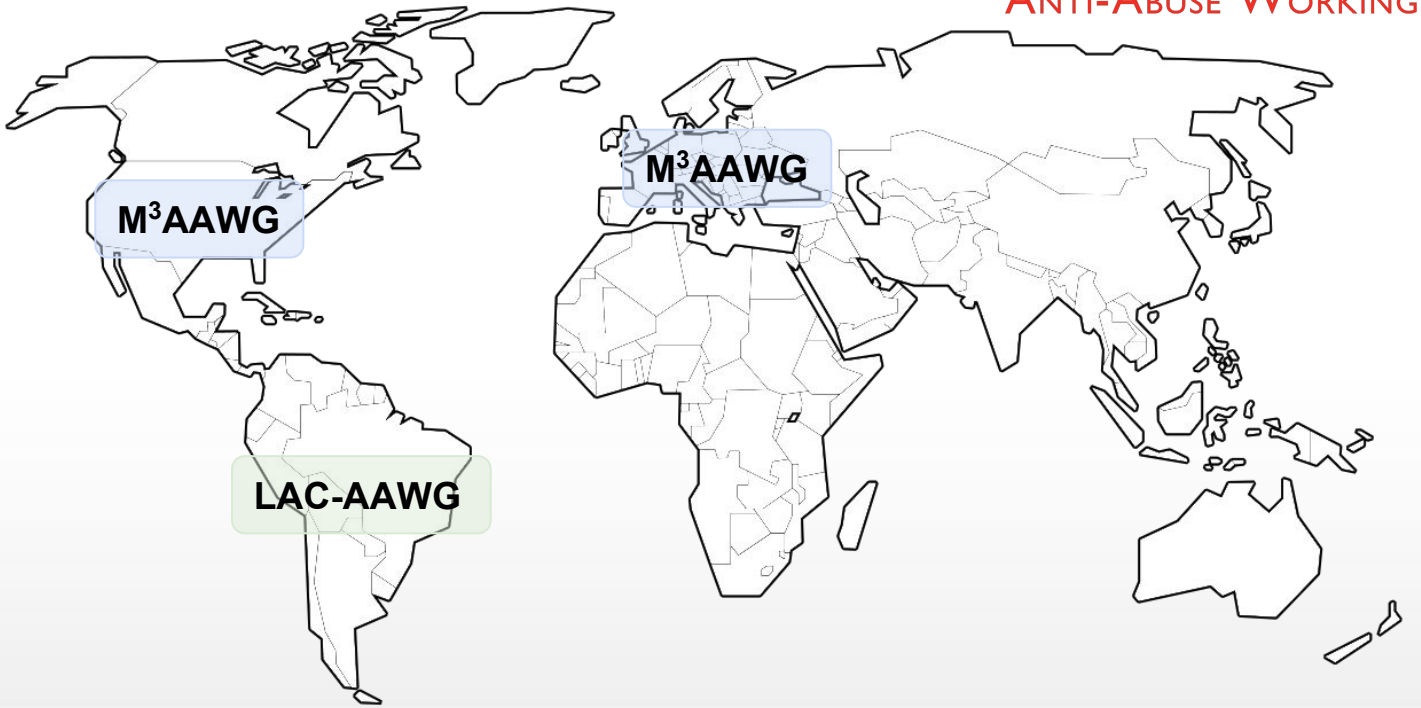
Outreach:
Anti-Abuse Working Group (AAWG) Development

Regional AAWG Development
Contributing to *Peer* Working Groups

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Regional AAWGs Development
Contributing to *Peer* Working Groups

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group



Regional AAWGs Development
Peer Working Group in LAC

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

M³AAWG 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 M³AAWG 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, M³AAWG 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 M³AAWG 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 M³AAWG y su permanente trabajo en el

Regional AAWGs Development
Peer Working Group in LAC

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

LACNOG Anti-Abuse Working Group

Introduction:

In March of 2016 LACNIC and M³AAWG established a memorandum of understanding (MOU) to collaboratively combat "global cybersecurity issues" and "online threats" (reference). As part of this MOU, M³AAWG established its LAC Initiative to help develop a self-sustaining anti-abuse community in the LAC region. Strategically, this effort balances M³AAWG's historical expertise in anti-abuse efforts in North America and Europe with the nuanced difference in abuse dynamics in the LAC region. As part of this effort, M³AAWG is collaborating with LACNIC and LACNOG to develop the LACNOG Anti-Abuse Working Group, or LAC-AAWG.

LAC-AAWG Charter

LAC-AAWG will serve as a convening forum for operators in the LAC region that want to develop anti-abuse recommendations and best common practices (BCP) and global members

Regional AAWGs Development
Peer Working Group in LAC

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

AAWG Principles and Objectives

Promulgate anti-abuse norms and principles

Further develop regional anti-abuse expertise

- ➔ Anti-abuse research
- ➔ BCPs within and across regions

Convene anti-abuse actors

- ➔ operators
- ➔ public policy
- ➔ LE

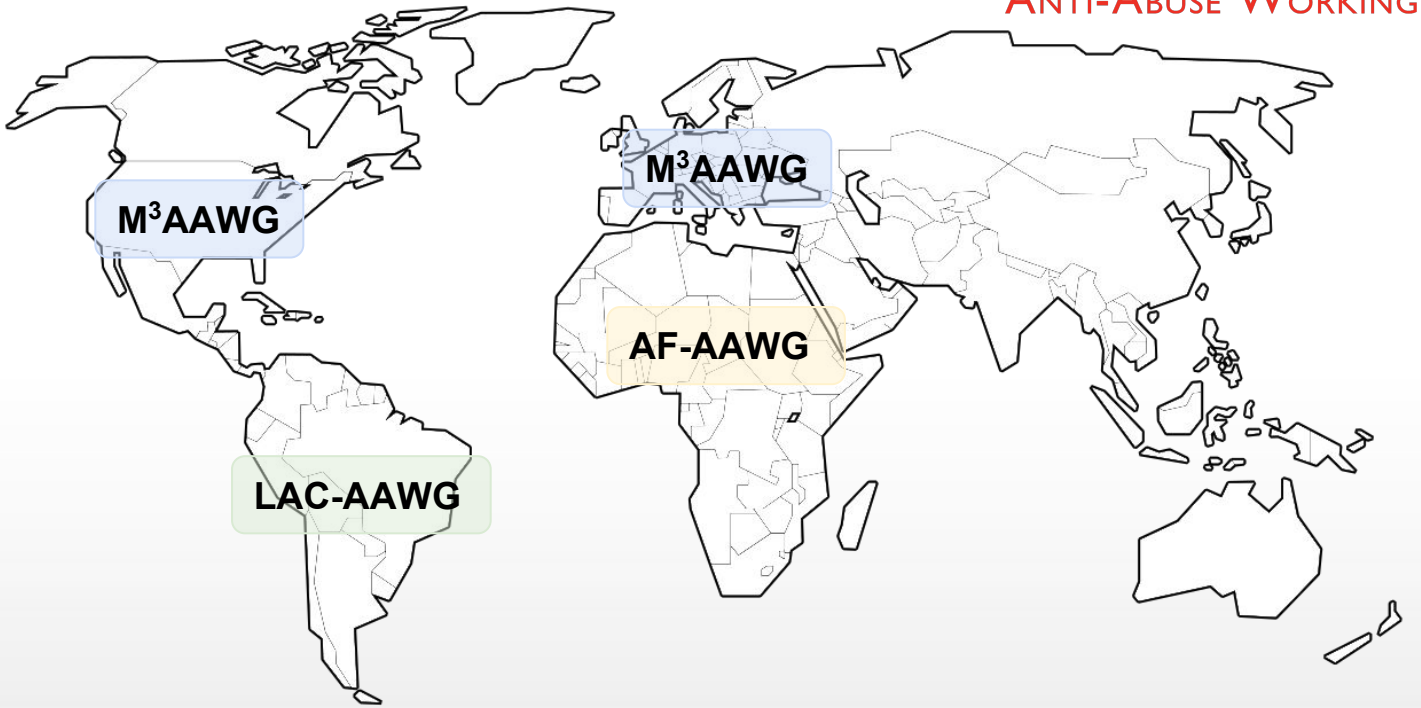
Represent regional anti-abuse expertise

Exchange expertise

- ➔ among operators within the regions
- ➔ globally, among peer regions

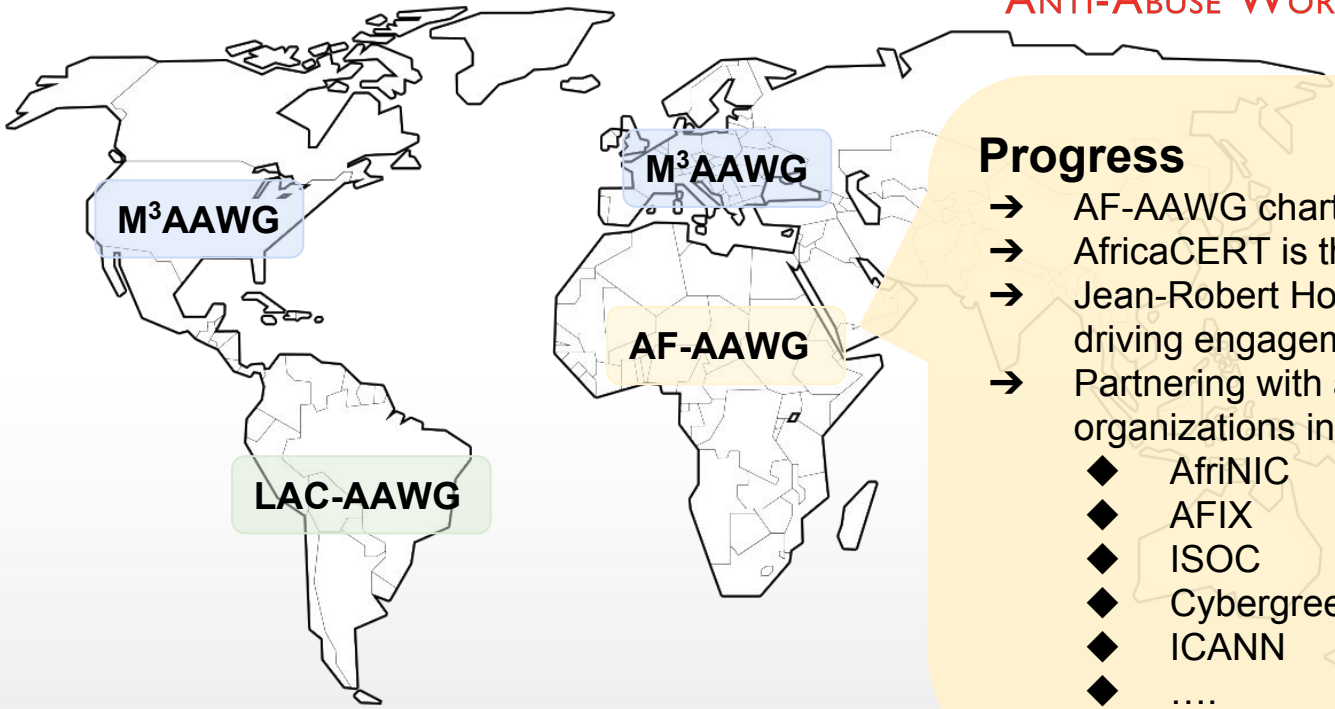
Regional AAWGs Development
Peer Working Group in AF

M³AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP



Regional AAWGs Development
Peer Working Group in AF

M³AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

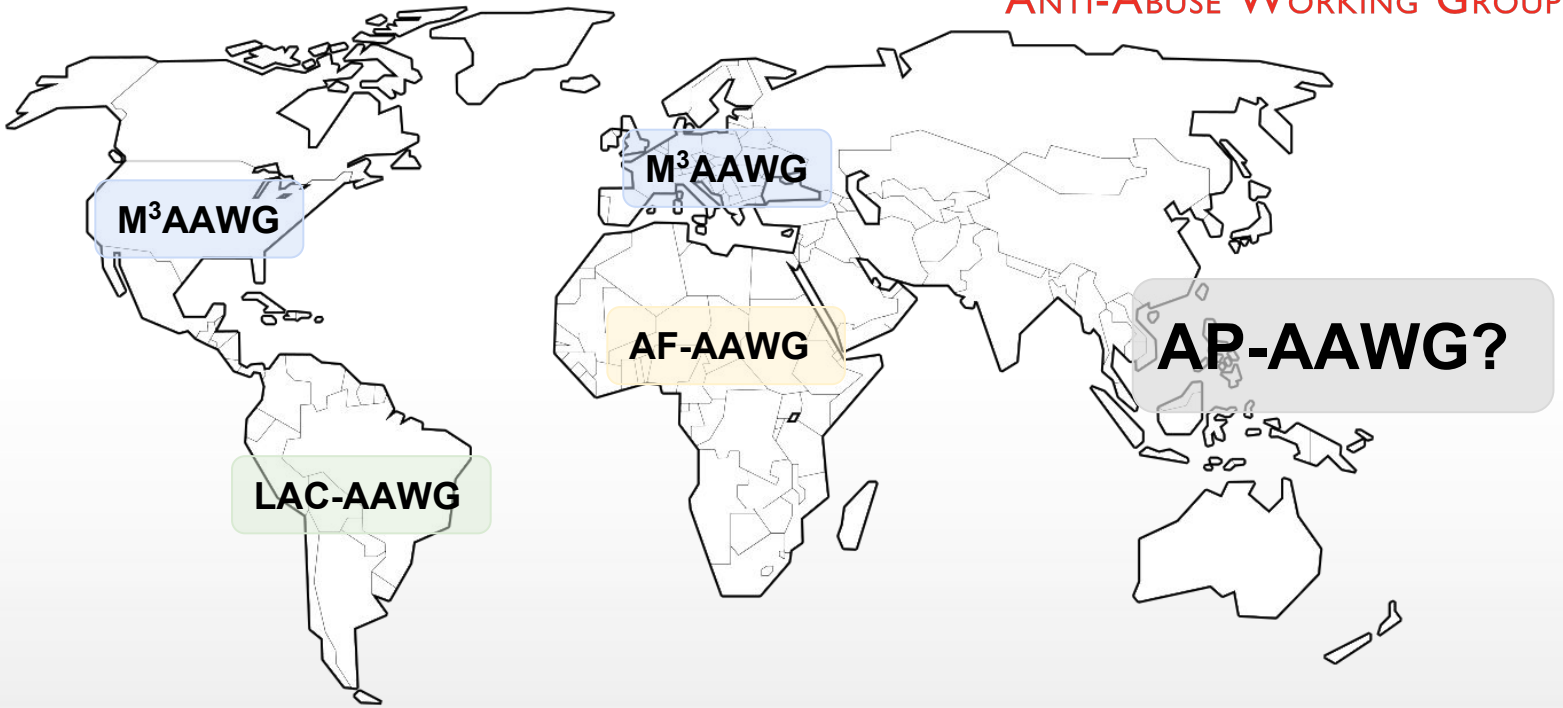


Progress

- ➔ AF-AAWG charter drafted
- ➔ AfricaCERT is the home
- ➔ Jean-Robert Hountomy is driving engagement
- ➔ Partnering with a variety of organizations including
  - ◆ AfriNIC
  - ◆ AFIX
  - ◆ ISOC
  - ◆ Cybergreen
  - ◆ ICANN
  - ◆ ….

Regional AAWGs Development
Peer Working Group in AP?

M³AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP



M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Questions?
Comments?
Volunteers?!?

jesse.sowell@gmail.com