



# Messaging, Malware and Mobile Anti-Abuse Working Group - M<sup>3</sup>AAWG

Jerome Cudelou, M<sup>3</sup>AAWG Vice Chairman



# Who is M<sup>3</sup>AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group



- The largest global industry and public policy organization working against bots, malware, viruses, denial-of-service attacks, other online exploitation and mobile abuse on current and emerging platforms.
- A technology-neutral, non-political working body, M<sup>3</sup>AAWG systematically focuses on all aspects of messaging abuse including technology, industry collaboration and public policy.
- It brings together all the players in the online community in a confidential, open forum to develop cooperative approaches for protecting consumers and promoting a safe online experience.
- M<sup>3</sup>AAWG covers over one billion inboxes with more than 200 members worldwide. [http://www.m<sup>3</sup>aawg.org/about/roster/](http://www.m3aawg.org/about/roster/)

## M<sup>3</sup>AAWG – Our Focus :



As an organization, we targeted abusive messaging, malware and mobile plus other new forms of abuse:

**Messaging** - we will continue to tackle abuse on any messaging platform, from email to texting, as we've always done.

**Malware** - because spam is just the symptom, like the spots that appear with measles. The real pathology is the bots, viruses and malicious code that surreptitiously infect users' systems. If we block the pathology – the malware – from accessing the system, the fraud and user vulnerabilities will dissipate.

**Mobile** – is the future and we need to protect this platform now, as it under attack with malware and messaging abuse – text and voice.

## Driven by ISPs & Technology Changes



- Membership Includes ISPs, Telecomm Companies, Email Providers
  - All Major U.S. ISPs: ATT, Comcast, TWC, Verizon, Cox, CenturyLink
  - Global Members Including 1&1 Internet AG, Bell Canada, Orange, Internet Initiative Japan (IIJ), Rediff.com India Ltd, Swisscom, TDC, Telenet N.V., UPC Broadband Operations BV, Yandex (Russia), XS4ALL Internet B.V.
  - Major Email Providers: AOL, Google, Microsoft, Yahoo!, 1&1, Mail.ru
  - U.S. Mobile Operators: ATT, Verizon Wireless, Sprint, T-Mobile
- Social Networking Companies & Major Brands
  - Facebook, LinkedIn, Twitter,
  - Amazon Web Services, PayPal, JPMorgan Chase, Rakuten
- Leading Hardware & Software Vendors
  - Apple, Cisco, IBM, Oracle, Adobe
  - All Major Antivirus Vendors and numerous Security Vendors

## Extensive Global & Industry Reach

- Many Nonprofit Members including
  - CAUCE; eco-Association of German ISPs; ICSI (Berkeley); Internet Systems Consortium (ISC); Internet Society (ISOC); Spamhaus; Shadowserver; SURBL; Team Cymru: REN-ISAC
- Concerned Government Entities
- Law Enforcement
  - London Action Plan (LAP) Member – M<sup>3</sup>AAWG Hosted Meetings
  - Invite-Only Law Enforcement Training & Sessions
- Members in North America, Europe, Asia, India, Russia
  - Outreach to China
  - M<sup>3</sup>AAWG India

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



- Develops & Publish Best Common Practices & Position Statements
  - Recommendations Not Rules
  - Encourages Reluctant Firms toward Accepted Practices
  - i.e., M<sup>3</sup>AAWG Port 25 BCP – Global Impact
- Many M<sup>3</sup>AAWG Papers Referenced in Standards
  - Bot Mitigation BCP is now IETF RFC6561
  - FBL BCP is now IETF RFC6449
- Technical Outreach to Global Partners
- Provides technical and operational guidance to government, Internet and public policy agencies developing new Internet policies and legislation. M<sup>3</sup>AAWG Papers Referenced in Government Reports.

## A Few Published M<sup>3</sup>AAWG Papers:



- Position on Email Appending
- Mitigating Abuse of Web Messaging Systems
- Complaint Feedback Loop Best Current Practices
- Email Anti-Abuse Product Evaluation Best Current Practices
- Overview of DNS Security - Port 53 Protection
- Mitigating Large Scale Bot Infections in Residential Networks
- Use of a Walled Garden  
(Chinese, French, Spanish Translations)
- BIAC-MAAWG Best Practices Expansion Document  
(Arabic, Chinese, French, Spanish Translations)
- Anti-Phishing Best Practices for ISPs and Mailbox Providers  
(Chinese, French, Spanish Translations)
- Managing Port 25 (French, German Translations)

## Sharing Knowledge & Exceptional Training Opportunities for Members

- M<sup>3</sup>AAWG provides a trusted forum & framework for open discussion of abuse issues in an atmosphere of confidentiality and cooperation.
  - Dialogue on Needs & Solutions within Industry
  - Information Sharing Among Trusted Sources
- Some Previous Training Topics:
  - Wireless & All IP Network Mobile Solutions
  - Advanced DNSSEC
  - Spamtraps
  - Malware Analysis
  - Visualization
  - Advanced Methods Used by SMS Spammers




## Outreach initiatives



- EWI Chose M<sup>3</sup>AAWG for China Exchange
  - Feb. 2011: EastWest Institute Announces “Building Trust through Cooperative Technology” at M<sup>3</sup>AAWG (Released June 2011)
  - June 2011: M<sup>3</sup>AAWG Chaired Sessions at EastWest Institute London Summit; EWI Hands-Off Chinese Work to M<sup>3</sup>AAWG
  - Aug. 2011: M<sup>3</sup>AAWG Speaks at China National Computer Network Emergency Response Team (CNCERT) Annual Conference
- India Outreach
  - Initial workshop sponsored by Internet Security Council of India
  - Ongoing Meetings in India and Other Outreach to Indian ISPs
- EastWest Institute 2013 Cyber Security award for China & India work
- M<sup>3</sup>Anti-Abuse Foundation (m3aaf.org) – championed an independent nonprofit dedicated to anti-abuse training in developing online countries

## New initiatives

- Voice and Telephony Abuse Special Interest Group 
  - Telephony is becoming another Internet medium for cybercriminals to exploit - inexpensive VoIP services provide accessibility and anonymity for global abuse.
  - 1st Workshop Feb. in San Francisco & 2nd Workshop June 18-19 in Montreal
  - M<sup>3</sup>AAWG Brussels June 9-12 a update session for interested new participates.
- Hosting Special Interest Group
  - Addresses issues with cloud storage security, identifying and removing illegitimate accounts, and protecting hosting servers against DDoS and other attacks
  - Initial best practices paper in draft with numerous hosting companies and other industry partners. Two working sessions set for M<sup>3</sup>AAWG Brussels meeting.
- Pervasive Monitoring Special Interest Group
  - Evaluating the technical aspects of higher security levels that may also reduce the ability to mitigate online abuse.
- Abuse Desk Special Interest Group
- Update of OECD Best Practices to Address Online and Mobile Threats developed by M<sup>3</sup>AAWG and London Action Plan

# Thank You



- Thank you for your interest
- If you want more information on our work or our organization please contact us at [http://www.m3aawg.org/contact\\_form](http://www.m3aawg.org/contact_form)
- If you want to attend one our meetings and participate in the work please contact Jerry Upton, Executive Director, at [jerry.upton@m3aawg.org](mailto:jerry.upton@m3aawg.org)
- M<sup>3</sup>AAWG Next Meeting: **31st General Meeting- Brussels, Belgium** - Sheraton Brussels Hotel - - Training June 9, 2014, General Sessions June 10-12, 2014
- All upcoming M<sup>3</sup>AAWG Meeting locations for 2014 and 2015 are posted at: [http://www.m3aawg.org/events/upcoming\\_meetings](http://www.m3aawg.org/events/upcoming_meetings)