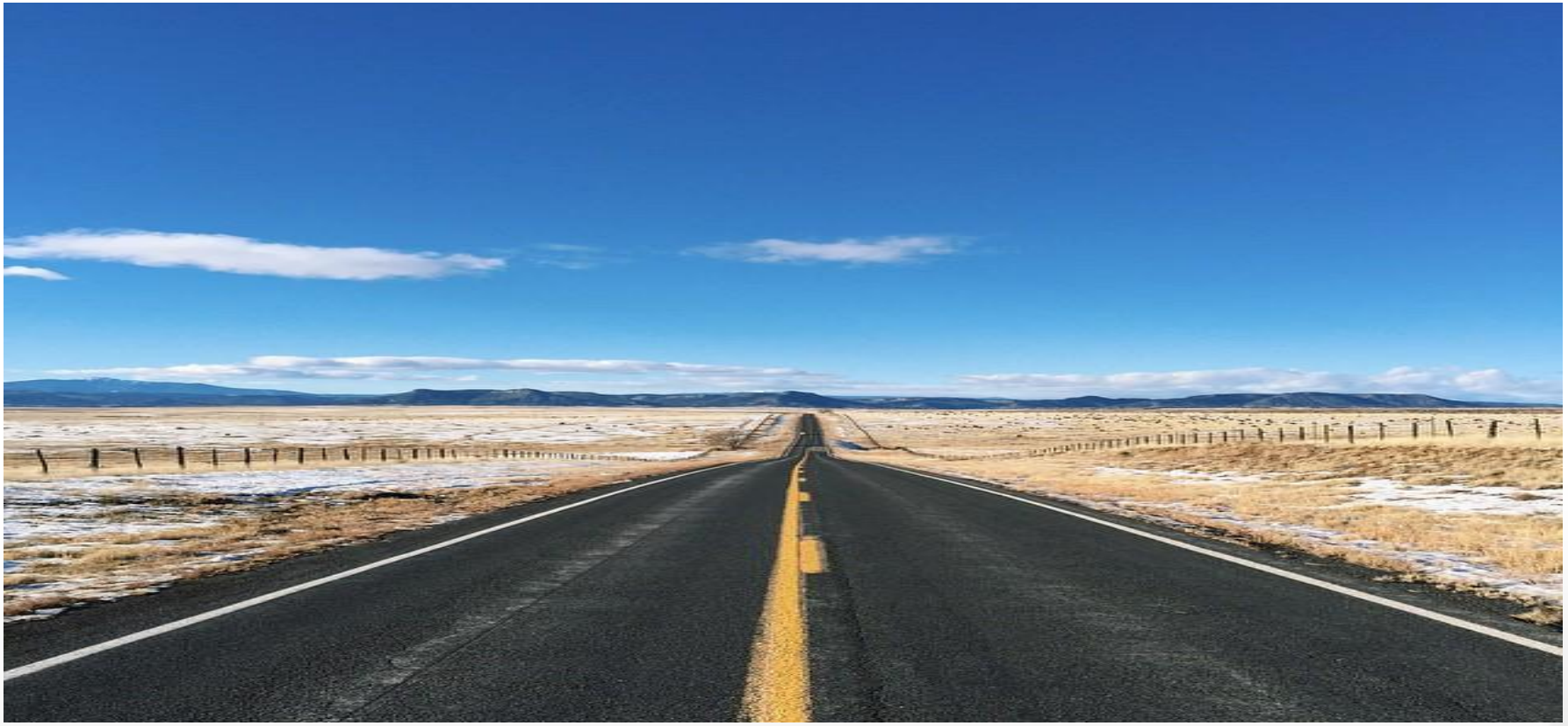
M³AAWG: Hosting Past, Present & Future

Justin Lane - BlueHost and M3AAWG Hosting Co-Chair
Jesse Sowell, PhD and M3AAWG Advisor

5 May 2016

LACNIC 25, La Habana, Cuba

Hosting: Not a Big Issue, Right?



For many years the Community looked at Hosting Companies like this picture. We where a small area that did not look to be that important.

A Brief History of Hosting

Hosting Companies in the beginning where a small part of the overall environment. Most of the Hosting Companies at the time offered plans that gave their clients 20-50MB of space to use for their websites.

ESP's and ISP's where much bigger players.

What Hosting Offers

Hosting Companies were able to offer all the services needed to get a company online and ready to service their customers.

- Email Services
- CMS, and Webdesign
- Hardware from Dedicated Servers or Colocation Servers to Shared or Virtual Server Space
- Bandwidth for your Business, Dedicated Ips and SSL Services
- Access to Hardware that most smaller businesses were not able to afford on their own.

What is Happening Today?

As the community got better at policing ISP's, ESP's and other problem areas, the criminal elements began to migrate to the Hosting Platforms.

With Hosting Companies these criminal elements were even better positioned to carry out their plans.

And in the beginning we were not prepared to address these problems.

Abuse in Hosting

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

A Hosting Company is the one stop shop for their customers needs in so many areas.
This also means Hosts are open to abuse from many different areas

- Spammers, creating spam campaigns.
- Hackers breaking into Customer sites.
- Being used as targets or sources for malware or botnet infections.
- Phishing sites.
- Child Exploitation.

What Happened Next

MAAWG recognized the need to address the problems that were developing in the Hosting Industry. And decided on a plan.

- Approach Hosting Companies to engage with the industry.
- Once engaged we created the Hosting SIG to address the problems Hosts face.
- Encouraged the Hosting Companies to design their Best Common Practices.
- With the help of industry experts we designed the Hosting and Cloud Best Common Practices

Why MAAWG Could Help

- **Provide a Trusted Forum & Framework for Open Discussion** of Abuse Issues in an Atmosphere of Confidentiality and Cooperation
- **Develop & Publish Best Common Practices & Position Statements**
  - Recommendations Not Rules
  - Encourages Reluctant Firms toward Accepted Practices
  - i.e., M^{3}AAWG Port 25 BCP – Global Impact
- **Many M^{3}AAWG Papers Referenced in Standards**
- **Technical Outreach to Global Partners** – London Action Plan and EastWest Institute (2013 Cyber Security Award for China & India Work)
- **Provide Technical and Operational Guidance to Government, Internet & Public Policy Agencies** Developing New Internet Policies and Legislation. M^{3}AAWG Papers Referenced in Government Reports.

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Hosting, What We Are Today.

Today, Hosting Companies Have a HUGE Impact on the Ecosystem. Because of all the various services that they offer.

The Basic services Hosting Companies offers their clients have not changed. But our technology has. Everything has improved, we are faster, stronger and larger than we ever thought possible. And as technology gets better we pass that on to our customers.

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

How Does M3AAWG Help?

Because you can't ***effectively*** or ***efficiently***
fight online abuse alone

Because you can't ***protect***
your end-users and customers in a vacuum

M3AAWG is a Global Trusted Community for Sharing Information, Techniques, Research

Our Urgency and Dedication

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Malware & Crime Have Intensified – Growth of the Underground Economy
- New Attack Vectors Identified Constantly
- Mobile in Cybercriminal's Sight

Today's Threats Require Multi-Discipline, Global Response

- Cut Across Fields of Specialty, Technologies, Silos
- Borderless Crimes Demand Global Cooperation
- Outreach to Developing Online Countries
- Shared Expertise and Proven Recommendations

What hosting Companies Need to Know

M3AAWG members have created BCPs that help simplify the issues.

These documents are designed so that it does not matter if the hosting company is one person working out of his house or a company of thousands, they can be used by anyone.

The goal is to make sure that the needed information is easy to understand and easy to start implementing.

How M³AAWG for Hosting Helps

"Participating in M³AAWG has made my job easier and made me more effective at my job" – Hosting Company Anti-Abuse Manager

- M³AAWG Members are Experts in Spam, Phishing, Malware
  - Areas of Urgent Concern to the Hosting Community
- Brings Together Needed Resources
  - Blacklisting Groups
  - Security Researchers Identifying Upcoming Threats
  - Colleagues Who Have Dealt with Threats
- Collaborate with Others Working on Similar Problems
  - Avoid Costly Trial and Error
  - Implement More Effective Anti-Abuse Measures

Contributing to Standards

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

- Provide Input into RFCs and Other Standards
  - RFC 6449 – Complaint Feedback Loop Operational Best Practice Recommendations
  - RFC 6561 – Recommendations for the Remediation of Bots in ISP Networks
  - RFC 6650 - [...] Abuse Reporting Format (ARF)
  - RFC 6376 (DKIM) and draft-kucherawy-dmarc-base-13.txt (DMARC) Have Substantial Input from M^{3}AAWG Members and Technical Advisers

Hosting Vital to Ecosystem Health

Kicked Off Best Practices Work in 2014 – Published in Q1 2015

"We are thrilled to collaborate with M^{3}AAWG on this important best practices initiative and focus on implementation within this community."
Christian Dawson, i2C chairman and co-founder

"We took on this work at M^{3}AAWG because of the pivotal role hosting companies play in the ecosystem . . ."
Michael Adkins, M^{3}AAWG Chairman of the Board

M³AAWG Anti-Abuse BCPs for Hosting and Cloud Service Providers

- See www.m3aawg.org - Best Practices
- Jointly Published by the i2C and M³AAWG to Reduce Spamvertising, Malware, Other Online Threats
- Outlines Needed Hygiene and Security to Improve Operations and Better Protect End-Users
- Reasonable Steps that Can Be Integrated into a Company's Basic Operations and Policies
- Developed by Industry Professionals Facing These Challenges Every Day

How can the Hosting BCP Help?

Covers Types of Abuse, Prevention, Detection, Identification, Remediation

- Institute Effective New Client Vetting Before Allowing Customers on Your Network
- Require Customers to Keep Current on All Software Updates
- Consider Hardware-based Intrusion Detection Systems (IDS)
- Use Software-based Security Scans and Firewalls
- Implement Internal Network Telemetry Reporting
- When a Problem Is Found, Best Practices Recommend When to Suspend Service or Terminate Customer
- Use Network Operators' Feedback Loops to Identify Abusive Email Sent from Your Service and Help Identify Potential Problems

Where to Start?... Prevention!

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

Vet customers before they can cause a problem!

Hosting providers are at the mercy of their clients' worst practices. Providers must have some type of vetting process to proactively identify malicious clients before they undertake abusive activities. A sound vetting process prior to provisioning will help the provider determine the difference between the truly bad actors and the customer who simply needs some guidance on proper online conduct. Vetting of clients is integral to maintaining a good reputation, decreasing costs and decreasing online abuse.

What Comes Next? Education!

You and your teams need to know what threats to watch out for. The only problem with that is that the threat landscape is constantly changing.

Thankfully none of us are alone in this battle. It is essential that lines of communication are set up with reputable reporting groups to help maximize your ability to correct problems as they occur.

M³AAWG Resources

- M³AAWG Website
  - Exclusive Members-Only Documents and Resources on the Members Section of Website
- Public Accounts - Anyone (members & non-members) can access these:
  - YouTube Channel - www.youtube.com/maawg.
  - Twitter - @maawg – www.twitter.com/maawg
  - Facebook Page - https://www.facebook.com/MAAWG
  - Google+ page - search for maawg
- Private Groups - M³AAWG members are welcome to join:
  - Facebook Group - www.facebook.com/groups/maawg
  - LinkedIn Group – M³AAWG

Some Current Threats

SnowShoe Spammers - Currently one of the hardest threats for Hosting Companies to combat.

Why?

Because most of these spammers will open multiple accounts with Hosting Companies and then do nothing with them. For a while, once they start using those accounts they are not flooding outbound MTAs they are only sending a few hundred emails. This while it may be caught does not match the normal profile of a spammer.

SnowShoe Spammers

Current Best Practices for combating these issues.

- Vetting your new customers. Using strict vetting practices and maintaining data on past problem customers. The additional bonus of having strict Vetting policies is a lower amount of fraudulent accounts across the board.
- Third party reports. Because of the relatively small amount of mail sent from these types of spammers, it is essential to have trusted feedback sources. They maintain large networks of honeypots that help identify these trends.
- Limit the access new customers have to the system. Setting limits for emails sent per hour with a new customer is one example of how to prevent some of the problems at the outset.

Current Threats Continued

- Malware and Botnets
- Phishing
- Virus Payloads

Combating these Threats, once again starts with proper vetting. Your Feedback loops will also be a major point of contact to help combat these issues.

Internal systems designed to check for malware, botnet , phishing etcetera is another needed process to secure your network.

Finally educating customers on proper security, for their accounts and home pc's.

Hosting Committee - Our Purpose

Addresses Issues with Cloud Storage Security, Identifying and Removing Illegitimate Accounts, Protecting Hosting Servers Against DoS and Other Attacks

Why M³AAWG for Hosting Works

- M³AAWG Members Experts in Spam, Phishing, Malware
  - Areas of Urgent Concern to the Hosting Community
- Brings Together Needed Resources
  - Blocklisting Groups
  - Security Researchers Identifying Upcoming Threats
  - Colleagues Who Have Dealt with Threats
- Collaborate with Others Working on Similar Problems
  - Avoid Costly Trial and Error
  - Implement More Effective Anti-Abuse Measures

Up And Coming Threats

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

The Cloud

Cloud Hosting

Cloud Technology has dramatically changed the landscape for Hosting Companies. While the Virtual Hosting Environment has dramatically increased the services Hosts can offer their clients, it is also bringing with it new types of abuse.

With the Cloud, a server can easily be spun up in minutes, be provisioned and online ready to go to work.

Abuse in The Cloud

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

We have already started to see some of the possible abuse scenarios, Targeted Phishing or Spam Campaigns that are up for a relatively short time, then the server is deleted and gone from a Host's system.

Currently we are in the process of updating the BCP to reflect the issue we are just discovering that affect the cloud.

Working with Abuse Reporters and Hosting Providers we are trying to address the new abuse vectors.

How The Process Works

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

By Bringing Reporters and Providers together we are able to create a realistic picture of the problem and formulate an acceptable response.

Usually neither side gets everything they want, however they usually get what they need.

When looking at the problem of overall response time to abuse reports by Hosting Companies. We have tried to come at the problem from multiple sides.

Currently we have two initiatives that are addressing this.

What you could Normally see.

Reporter: “Hosting Companies are just ignoring my reports. It has been three days and the problem is still up.”

Host: “Today I only have 3,000 new abuse reports! And none of them are in the same format!”

Both groups have legitimate problems. Working together we try to address these issues and create real solutions.

Exploring Solutions

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

- **Report Format for Inbound Phishing Reporting (LARTS)**
  A Policy Paper on Formatting Proper Complaint Submissions
- **Pilot to Improve the Effectiveness and Actionability of Exploit Reports**
  Jointly with M3AAWG Brand SIG

These projects are designed to improve response time for both sides. By having standard reporting formats it opens the possibilities for Hosting Companies to automate many types of reports.

Dedicated trusted reporters allows Hosts to respond faster with a greater degree of trust.

Hosting Committee
Ongoing and Future Work

- **Expanding our Current BCP with regards to Cloud Hosting.**
- **DNS Provider Best Practices**
  Phase Two of Our Best Practices Work
- **Port 25 for Hosting Companies**
  Possible Policy Paper
- **Report Format for Inbound Phishing Reporting (LARTS)**
  A Policy Paper on Formatting Proper Complaint Submissions
- **Pilot to Improve the Effectiveness and Actionability of Exploit Reports**
  Jointly with M^{3}AAWG Brand SIG

A Few Published M³AAWG Papers:

- M³AAWG/LAP Operation Safety-Net Global Best Practices
- Mobile Messaging Best Practices for Service Providers
- Anti-Abuse BCPs for Hosting & Cloud Service Providers
- TLS for Mail: M³AAWG Recommendations
- Benefits and Deployment of Telephony Honeypots
- Position on Email Appending
- Anti-Phishing Best Practices for ISPs and Mailbox Providers (updated)
- Mitigating Abuse of Web Messaging Systems
- Complaint Feedback Loop 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)
- Managing Port 25 (French, German Translations)

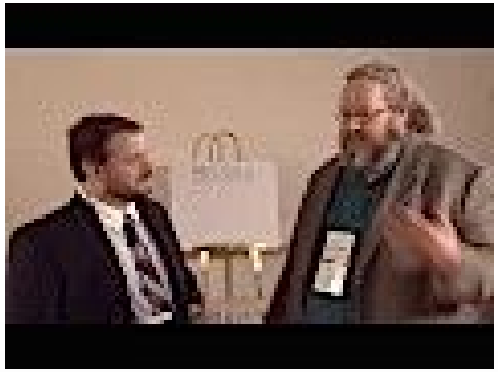
Hosting Videos

www.youtube.com/maawg

See Hosting Playlist on M³AAWG YouTube Channel

Outlining Hosting Best Practices

Improving Your Business with the M³AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers



Value of M³AAWG to Hosting Companies

How the M³AAWG Hosting SIG Can Help You; Fighting Spam, Phishing, Malware and Emerging Threats

M3AAWG MEETINGS

For More information please contact:

Fabricio Pessoa
fabricio.pessoa@axur.com

Graciela Martinez
gmartinez@lacnic.net

Meeting Schedule
http://www.m3aawg.org/upcoming-meetings

M3AAWG 37th General Meeting

Where:
Sheraton Downtown Philadelphia
Philadelphia, USA

When:
Training June 13, 2016
Members Sessions June 14 - 16, 2016

Hotel Information | Agenda | Online Registration not open

M3AAWG Meeting Calendar

2016 Dates and Locations

38th General Meeting
October 24-27, 2016, Paris, France
Training Oct. 24
Members Sessions Oct. 25-27
Paris Marriott Rive Gauche Hotel

2017 Dates and Locations
39th General Meeting
February 20-23, 2017, San Francisco, California, USA
Training Feb. 20
Members Sessions Feb. 21-23
Palace Hotel

40th General Meeting
June 5-8 or 12 -15, 2017, Europe
Hotel TBD

41st General Meeting
October 2-5, 2017, Toronto, Canada
Training Oct. 2
Members Sessions Oct. 3-5
The Westin Harbour Castle, Toronto