

The logo features the text 'M3 AAWG' in blue, with 'M3' enclosed in a blue square. Below it, 'ENGAGEMENT SERIES' is written in red. The logo is centered within a white circle that has a thick blue border and a red inner ring. The background consists of several overlapping circles in shades of blue and red, some containing a white hexagonal molecular pattern.

M³ AAWG
ENGAGEMENT SERIES

All About the AAWGs

JPAAWG, AFAAWG, LACAAWG

Supported by the
Growth & Development Committee

October 24, 2023

M³AAWG is a Trusted Environment

What happens in M³AAWG stays in M³AAWG

- What occurs here cannot be shared outside the membership without the written permission of the Executive Director, unless we state the specific session is open to the press and social media.
- See the M³AAWG Meeting Policy at www.m3aawg.org/MeetingPolicy

Treat Everyone with Respect

- Treat all attendees respectfully in and out of sessions. No less will be tolerated.
- See the M³AAWG Conduct Policy at <https://www.m3aawg.org/conduct-policy>

You agreed to these policies when you registered for the meeting.
For questions, please contact Amy Cadagin at amy@m3aawg.org

Reminders for Our Worldwide Friends

All meeting content is confidential: No photos, no video, no recording. Reach out to staff with questions.



L'ensemble du contenu de la réunion est confidentiel : les photos, vidéos et enregistrements sont interdits. Pour toute question, demandez conseil au personnel.



Todo el contenido de la reunión es confidencial: No está permitido sacar fotografías ni grabar vídeo o audio. Consulte con el personal si tiene alguna pregunta.



Der gesamte Inhalt des Meetings ist vertraulich: Keine Fotos, kein Video, keine Tonaufzeichnung. Bei Fragen wenden Sie sich an die Mitarbeiter.



会議の内容はすべて機密扱いです。写真やビデオの撮影、録音は禁止されています。質問がある方は、スタッフまでご連絡ください。



所有会议内容均为保密信息：禁止拍照、录像、录音。如有疑问，请咨询职员。



회의에서 다루는 모든 내용은 기밀입니다. 사진 및 동영상 촬영과 녹음은 금지됩니다. 질문이 있으시면 직원에게 문의해 주십시오.



Все содержимое собрания является конфиденциальным: нет фотографий, нет видео, нет записи. Смотрите сотрудников с вопросами.

Growth & Development | Mission & Vision

Vision - Why We Exist

The M³AAWG Growth and Development Committee believes in and is working towards **a world free of online abuse through collaboration** - sharing our knowledge, assets, and network with others.

Mission - What We Intend To Be

We will be the collaborative leader, facilitator, and stakeholder for alignment, support, and execution of anti-abuse best practices through a global network of partners fighting online abuse on all platforms.

AF-AAWG Overview



Brian Scriber

CableLabs

b.scriber@cablelabs.com

AFAAWG

- Primary contact: Jean-Robert Hountomey hrobert@africacert.org
- Objective: Anti-Abuse Efforts from M³AAWG:
 - Within countries and organization across the continent
 - From African countries and orgs to peering points
 - Traffic management
 - Network resiliency
 - Collaboration with other organizations
 - Communication of threats and mitigations



AFAAWG

- Building the MOU between M³AAWG and AF-AAWG
- Incorporating AFAAWG into the Coalition for a Digital Africa initiative: <https://coalitionfordigitalafrica.africa/#partners>
- April 2023: Joint AfricaCERT and FIRST presentation on IoT Botnets, DDoS, and Ransomware in Kigali, Rwanda by Brian Scriber
- Sept 2023: AIS presentation on DDoS given by both Rich Compton and Barry Greene.
- Nov 2023: Regional Cybersecurity Summit for Africa: present separately on network resiliency and IoT Security in Kampala, Uganda - Brian Scriber

AFAAWG

M³AAWG Opportunities:

- Dialogue and relationships with anti-abuse professionals in Africa and the Middle East.
- Show global engagement reach to regulators

Where Can You Engage?:

- Presenters
- AF-AAWG Projects
- Names/Numbers
- Coalition for a Digital Africa



Contact

For additional questions, please email:

[<growth-development-chair@mailman.m3aawg.org>](mailto:growth-development-chair@mailman.m3aawg.org)

JPAAWG Overview

Shuji Sakuraba

Senior Research Engineer

Internet Initiative Japan Inc. (IIJ)

Chairperson of JPAAWG

Deputy Chairperson of ASPC (Anti-Spam mail Promotion Council)

Chairperson of Anti-Spam Committee in Internet Association Japan (IAJapan)

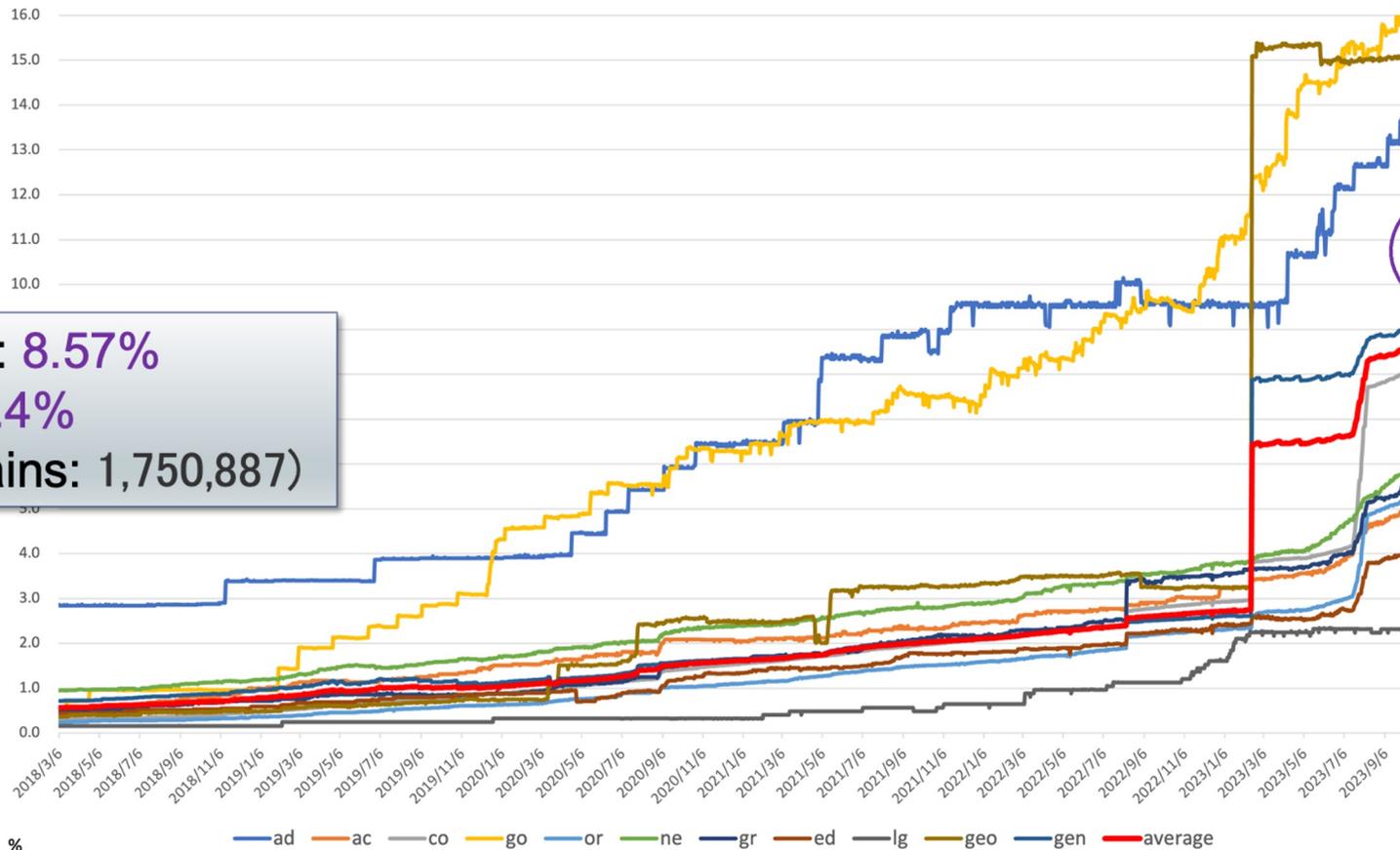
Ph.D.



JPAAWG

- Industry Working Group for **Safety and Security** of the Internet and Telecommunications
- Collaborate with government, academia and other related organizations (IAJapan, Council of Anti-Phishing Japan, ASPC, JANOG, etc)
- Founded in 2019, **JPAAWG General Meeting** has been held since 2018.
- Our current members are 20 companies, activities in cooperation with related major companies (mobile, telecommunications carriers)

JPAAWG



DMARC: 8.57%
SPF: 82.4%
(jp domains: 1,750,887)

Average:
8.57%

JPAAWG

- 6th General Meeting
 - **Date:** 6th-7th, November, 2023
 - **Venue:** Kanawaza City Bunka Center @ Kanazawa + Online
 - **Outline:** <https://meetings.jpaaawg.org/>
 - **Program:** 24 sessions (including 2 M3AAWG sessions), 2 Open Round Table Topics, 2 Training Sessions
 - **Registration:** <https://eventregist.com/e/JPAAWG6th> (Open!)



JPAAWG

- Interview Articles
- Flyer for GM



JPAAWG 6th General Meeting 注目プログラム

本講演、パネルディスカッションなど20以上のセッションが予定されています。

メールエンジニア/オペレータのためのCERT/PRECとの連携

Open Road Table T1S1.1の発表に際して

業界の若手・個人 Lightning Talks

M3AAWG / JPAAWG について

2023.11.6-7

金沢市文化ホール (石川県金沢市)

参加申し込み受付中!

<http://jpaawg.org/>

@ITSpecial

メールセキュリティ対策の第一—フィッシング、なりすまし—は最新動向を遡る

「メールを使ったサイバー攻撃を防ぐには受信者の協力が不可欠」——JPAAWGが議論の場を提供する理由

フィッシングなりすましメールを使ったサイバー攻撃は毎日のように発生しているが、メールセキュリティ対策は最新動向を遡る。そのうち、2023年7月、セキュリティ意識啓発の中で、自らセキュリティ課題に取り組み技術者同士の情報・意見交換を促す「JPAAWG 6th General Meeting」が開催される。JPAAWGはまさに、メールセキュリティの重要性とイベントの詳細について最新動向を、

2023年10月9日 19時00分 公開

印刷 共有

フィッシングやなりすましメールは増加傾向、不正送金被害額は2023年上半年で30億円

企業や個人を問わず、不特定多数が狙われるサイバー攻撃。データを暗号化して身代金を脅迫するランサムウェア攻撃や、IDやパスワードを窃取されたECサイトのアカウントに不正アクセスされる被害が、毎日のように報告されている。こうした中で、サイバー攻撃の基盤となるフィッシングメールはなりすましメールへの対応は急務とされている。

フィッシング対策協議会 事務局長 平塚伸世氏（一般社団法人JPCERTコーディネーションセンター）に話を聞いた。

「私も先日、著名なECサイトになりましたメールを受け取りました。『ご注文の確認』という文で、キャンセルするにはIDとパスワードを入力して確認するよう促されました。普段利用しているサービスだと、うっかり入力するようになります。また、最近IDやパスワードもログイン通知や注文確認、請求金額の通知など、さまざまなメールを送っています。サイバー攻撃者はそれらの正規メールの文面をコピーして、なりすまして攻撃を仕掛けてくるので、見分けがつかないという特徴があります。（平塚氏）

フィッシングメール自体も増加傾向にある。インターネットシニアディブの今村徳氏（ネットワーク本部アプリケーションサービス運用技術課）に話を聞いた。

「顧客やフィッシング対策協議会が公開している各種情報をよく読むと、かなり多岐にわたる。これはフィッシングメールが増えていると分かります。メール事業者や企業も、メールアドレスの機能追加やメールアドレス、対策に出していると思います。（今村氏）

2023年8月9日には警察庁が「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増」と題した注意喚起を公表している。2023年上半年における被害件数は、過去最多の2322件、被害額は約30億円に達していた。

ScanNetSecurity.jp 2023.10.09 (月)

HOME 脅威 脆弱性 情報漏えい インシデント 不正アクセス 報告書 講演 業界 新

検索

研修・セミナー・カンファレンス

2023.10.3 10月 8日

メールを軸に、インターネットの安全をさまざまな角度で知り、議論する「JPAAWG 6th General Meeting」の見どころとは

JPAAWG 6th General Meetingでは問題意識に立ち、課題解決の糸口を探り、前進させるさまざまなセッションが予定されている。M3AAWGのメンバーが笑日する他、通信事業者、企業、そして官公庁などさまざまな立場からスピーカーを招いたセッションを行う予定です。

JPAAWG

TOP OUTLINE PROGRAM PRIVACY POLICY ACCESS

フィッシング・サイバー脅威の最新動向について大手企業続々登場!

JPAAWG 6th General Meeting

2023.11.6 ~ 7

会費 + オンライン開催

企業で抱える課題をこの場でディスカッションしよう!!

「お支払い情報の再確認が必要です」「アカウント異常のお知らせです」——誰もが知る大手オンラインショップや金融機関を騙って受信者をだますとする、こんな迷惑メールが後を絶たない。残念ながらその文面にだまされ、クレジットカード番号をはじめとする個人情報を取られたり、マ

<https://atmarkit.imedia.co.jp/ait/articles/2310/06/news002.html>

<https://scan.netsecurity.ne.jp/article/2023/10/03/50023.html>

Contact

For additional questions, please email:
<contact@jpaawg.org>

LAC-AAWG

Lucimara Desiderá

Security Analyst, CERT.br / NIC.br

**LAC-AAWG Chair (a working group of
LACNOG)**

LAC-AAWG

- A Working Group of LACNOG, the Latin American and Caribbean Network Operators Group
- Main audience: the Latin American and Caribbean Network Operators community
- Create awareness regarding network/Internet abuse issues and foster de adoption of anti-abuse best practices
- Bring to M3AAWG some view of regional threats and efforts
- Collaboration with other organizations
- Established in 2017
- Published a joint BCOP with M3AAWG in may 2019

LAC-AAWG (most recent activity)

- During LACNIC40 – LACNOG 2023 (October 2023)
Identifying Spoofed DDoS Amplification Request Traffic in Your Network
by Rich Compton

lacnic 40
lacnog 2023
7-8 October / 7-8 Octubre 2023

Next Steps?

- Get more ISPs/IXCs to look for spoofed amplification traffic on their network!
 - It's not hard to find this traffic!
- Encourage offenders to clean up their networks!

Confidential to M3AAWG Members

lacnic lacnog nic.br cgi.br

Guest Presentation by the Anti Abuse Working Group LAC AAWG

<https://lacnic40.lacnic.net/en/programme/agenda/lacnog?day=03/10/2023>

<https://www.computerweekly.com/br/tip/Como-identificar-o-trafego-de-ataque-DDoS-na-rede-corporativa>

ComputerWeekly.com.br

Como identificar o tráfego de ataque DDoS na rede corporativa?

Um especialista explicou, durante o primeiro dia de atividades do LACNOG 2023, como o tráfego proveniente de ataques de negação de serviço pode ser detectado e compartilhou algumas ferramentas que podem ajudar nesta tarefa.

por Lizzette B. Pérez Arbesú, Editora Executiva para a América Latina Publicado: 03 out 2023

f
t
in
p
e

Fortaleza, Brasil. – No âmbito do evento [LACNIC 40](#), que acontece esta semana em uma praia do norte do Brasil, estão sendo realizadas sessões de trabalho do Grupo de Operadores de Rede da América Latina e do Caribe ([LACNOG](#)).

Entre as apresentações do LACNOG 2023, destaca-se a conferência de Rich Compton, membro do Grupo de Trabalho Anti Abuso (LAC-AAWG), que falou remotamente sobre como identificar o tráfego correspondente a ataques de negação de serviço (DDoS) de endereços falsificados em a grade.

Rich Compton é especialista em [detecção e mitigação de ataques DDoS](#), controle de botnets, segurança BGP e é responsável por manter a infraestrutura de rede segura na Charter Communications, onde trabalha atualmente.

Contact

For additional questions, please email:
lucimara@cert.br



Q&A

Place your questions in the Q&A Box below

Tip: To magnify the speaker's video, move the Zoom slider to the left.

Inquire how Your Company Logo Can Appear HERE:

sponsorship@m3aawg.org

Thank you!

We hope you enjoyed today's session!