News Release -Spanish

For Immediate Release

M³AAWG lanza serie completa de videos de entrenamiento de DMARC para combatir el spoofing de e-mail

SAN FRANCISCO, CA--(Marketwire - February 5, 2013) - A medida que la especificación de autentificación DMARC (Autenticación de mensajes basada en dominio, informes y conformidad), gana una adopción más amplia, el M³AAWG lanza una serie de videos gratuitos para ayudar a la industria a implementar y comprender el valor de la tecnología anti-phishing (delitos encuadrados dentro de las estafas cibernéticas). La serie de entrenamiento DMARC del M³AAWG ofrece cerca de dos horas y media de instrucción de expertos técnicos de la DMARC.org, incluyendo información para ambos propietarios de dominio que deseen proteger sus marcas contra el "spoofing" y para los ISPs o proveedores de casillas postales que deseen proteger a los usuarios finales de los mensajes fraudulentos.

La serie de entrenamiento de DMARC de M³AAWG incluye seis segmentos de 15 a 40 minutos originalmente presentados como una sesión de entrenamiento por Michael Adkins, covicepresidente de M³AAWG y socio de DMARC.org y Paul Midgen, presidente de DMARC.org, durante una reunión de M3AAWG en octubre de 2012. La serie ofrece los antecedentes generales acerca de la especificación DMARC y su propósito sobre cómo implementar la tecnología, y los detalles en sus procesos de informes.

La serie también incluye una sesión en grupos que aborda los temas relacionados específicamente a los propietarios de dominio y terceros que envían e-mails a otras empresas, y otras sesiones en grupos centradas en las cuestiones de ISP y proveedores de casilla postal. Los vídeos enfatizan consideraciones prácticas con Adkins y Midgen proporcionando numerosos ejemplos. La serie de entrenamiento completa DMARC de M³AAWG está disponible en el sitio M³AAWG bajo la pestaña de actividades de la página de vídeos de entrenamiento (https://www.maawg.org/activities/maawg-training-series-videos).

"El M³AAWG fue fundamental para el desarrollo de DMARC en su reunión y hoy que la tecnología está en etapa de adopción, continua apoyando la tecnología con el lanzamiento de esta serie completa de entrenamiento en vídeo. DMARC fue desarrollada para ayudar a las marcas y proveedores de casilla postal a trabajar conjuntamente en la identificación de mensajes fraudulentos. Estos videos son únicos debido a que son presentados por los expertos técnicos que ayudaron en el desarrollo de DMARC que explican cómo implementar la tecnología para obtener los mejores resultados", dijo Trent Adams, presidente de DMARC.org.

AOL, Gmail, Hotmail, Yahoo! y otros receptores de email utilizan DMARC para proteger a los usuarios finales y las marcas. La tecnología incorpora las especificaciones ampliamente utilizadas SPF y DKIM, sin embargo también incluyen retroalimentación, monitoreo y procesos de depuración, según Adams.

Chris Roosenraad, copresidente de la M³AAWG, dijo "Echando una mirada al contenido del mensaje, es generalmente imposible para los usuarios darse cuenta de que un email que parece provenir de su banco o su tienda favorita en realidad es una estafa, un intento de un delincuente de estafar al usuario. La práctica de spoofing (suplantar) o hacerse pasar por una marca conocida en un e-mail o engañar a los usuarios con su información personal u otros objetivos delictivos, es un problema cada vez mayor. Produjimos la serie de vídeo por cuanto los esfuerzos cooperativos como DMARC son esenciales para combatir este tipo de abuso y proteger a los usuarios".

Acerca del Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

El Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG - Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móvil), es donde se une la industria para trabajar contra los bots, malware, spam, virus, ataques de rechazo de servicios y otras formas de explotación en línea. El M³AAWG (www.M3AAWG.org) o M³ para mensajes, malware y móvil, representa más de mil millones de casillas de mensajes de algunos de los principales operadores de redes en el mundo. Aprovecha el alcance y experiencia de sus socios globales para abordar el abuso en las redes existentes y nuevos servicios emergentes a través de tecnología, colaboración y políticas públicas. También trabaja para educar a los formuladores de políticas globales acerca de los asuntos técnicos y operacionales relacionados con el abuso y mensajes online. M³AAWG con sede en San Francisco, California, es un foro abierto impulsado por las necesidades del mercado y respaldado por los principales operadores de redes y proveedores de mensajes.

Directorio de M³AAWG: AT&T (NYSE: T); Cloudmark, Inc.; Comcast (NASDAQ: CMCSA); Constant Contact (NASDAQ: CTCT); Cox Communications; Damballa, Inc.; Eloqua; Facebook; France Telecom (NYSE and Euronext: FTE); Google; PayPal; Return Path; Symantec; Time Warner Cable; Verizon Communications; y Yahoo! Inc.

Socios plenos de M³AAWG: 1&1 Internet AG; Adaptive Mobile Security LTD; Adobe Systems Inc.; AOL; BAE Systems Detica; Cisco Systems, Inc.; Dynamic Network Services Inc.; Email Sender and Provider Coalition; Genius; iContact; Internet Initiative Japan (IIJ NASDAQ: IIJI); Mailchimp; McAfee Inc.; Message Systems; Mimecast; Nominum, Inc.; Proofpoint; Scality; Spamhaus; Sprint; y Twitter.
Una lista completa de socios está disponible en, http://www.m3aawg.org/about/roster.

Contacto de Medios:
Linda Marcus, APR
1+714-974-6356 (Pacífico EUA), LMarcus@astra.cc
Astra Communications