# News Release -Spanish

**For Immediate Release**

## M³AAWG publica nuevas mejores prácticas DKIM tras revelarse la vulnerabilidad de la longitud de clave

SAN FRANCISCO, CA--(Marketwire - November 7, 2012) [Actualizado: Dic. 11, 2013] - Con la capacidad recientemente revelada de falsificar mensajes de correo electrónico de las empresas que están utilizando claves de cifrado obsoletas y débiles para autenticar sus mensajes electrónicos, el grupo M³AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group) exhorta a las compañías a que ajusten sus procesos DKIM de inmediato para mejorar las salvaguardas de los usuarios finales. Además acaba de publicar nuevas mejores prácticas que abordan específicamente la vulnerabilidad. El M³AAWG hace un llamado a las empresas comerciales para que reemplacen las claves de verificación previamente seguras de 512 y 768 bits por un cifrado de 1024 bits y más alto, entre otras recomendaciones, para validar mejor la autenticidad de las personas que envían mensajes electrónicos.

"Hemos desarrollado un documento breve y conciso que explica las medidas relativamente simples e inmediatas que pueden tomar los remitentes de mensajes a gran escala para proteger sus marcas en respuesta a las preocupaciones recientes acerca de algunos niveles de cifrado y uso de claves. La tecnología avanza y para mantenerse a la par de los piratas informáticos, la industria debe revisar sus prácticas a la luz de su capacidad de expansión. Queremos que las compañías conozcan las rápidos cambios que pueden hacer para proteger a los consumidores y a sus marcas frente a este problema", dijo Chris Roosenraad, copresidente de M³AAWG.

"Mejores prácticas del M³AAWG para la implementación de DKIM a fin de evitar la vulnerabilidad de la longitud de clave", (www.maawg.org/sites/maawg/files/news/M3AAWG_Key_Implementation_BP-2012-11.pdf) detalla los pasos técnicos a seguir para abordar las vulnerabilidades actuales y está disponible en la sección "Documentos publicados" en el sitio de la organización en www.maawg.org/published-documents. Las recomendaciones incluyen:

- Actualización a una longitud mínima de clave de 1024 bits. Las claves más cortas pueden ser descifradas en 72 horas mediante servicios en la nube de bajo costo
- Rotación ~~trimestral~~ al menos dos veces al año [1]
- Fijación de firmas que caducan después del período actual de rotación de clave y revocación de claves antiguas en el DNS
- Uso del modo de prueba de clave solo por un corto tiempo y revocación de la clave de prueba después del "ramp-up"
- Implementación de DMARC en el modo de seguimiento y uso de DNS para controlar la frecuencia con que se consultan claves. DMARC (Autenticación de mensajes basada en dominio, informes y conformidad) es otra norma de uso frecuente junto con DKIM.
- Uso de DKIM más que de claves de dominio, que es un protocolo depreciado
- Trabajo con terceros contratados para enviar mensajes de correo electrónico de una empresa para asegurarse de que cumplan estas prácticas

DKIM es una norma de amplia aceptación utilizada por empresas, organismos gubernamentales, grandes proveedores de servicios de correo electrónico y otras entidades, que le permite a una organización asumir la responsabilidad por el envío de un mensaje de manera que puede ser validado por el destinatario. Por ejemplo, los servicios de correo electrónico, como AOL, Gmail y Yahoo, y las marcas comerciales implementan la norma como parte de su protocolo

de mensajería. La misma incluye una clave de cifrado en las cabeceras de los mensajes que los ISP y otros destinatarios utilizan para verificar que el mensaje fue en realidad enviado por la compañía en cuestión.

La implementación de DKIM dificulta la falsificación de mensajes de correo electrónico que parecieran ser enviados por una compañía reconocida, un engaño que utilizan a menudo los delincuentes para robar información de identificación personal a usuarios desprevenidos. A finales de octubre, el periodista de Wired Kim Zetter informó que muchas compañías estaban utilizando claves débiles de cifrado y otras prácticas cuestionables como parte de su implementación de DKIM, lo cual podría exponer sus mensajes electrónicos a esta posible falsificación por parte de los ciberdelincuentes.

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

Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) es el punto de reunión de la industria en su lucha contra bot, software maligno, correo indeseado, virus, ataques por denegación de servicio y explotación en línea. M³AAWG (www.M3AAWG.org) representa más de mil millones de buzones de correo de algunos de los mayores operadores de red del mundo. Aprovecha el alcance y la experiencia de sus miembros globales para abordar el abuso en las redes existentes y en nuevos servicios emergentes a través de la tecnológica, la colaboración y la política pública. También trabaja para educar a los encargados de formular políticas globales sobre los aspectos técnicos y operativos relacionados con el abuso y la mensajería en línea. Con sede en San Francisco, California, M³AAWG es un foro abierto impulsado por las necesidades del mercado y respaldado por los principales operadores de redes y proveedores de mensajería.

[1] **NOTA:** Cuando se publicó en 2012 el documento de "Best Practices", se recomendaba que las claves DKIM rotaran de forma trimestral. En trabajos posteriores, con los que se llegó a una versión más detallada del documento ("M3AAWG Best Practice") en lo que a estas rotaciones se refería, la recomendación se actualizó a una periodicidad mínima de dos veces al año. Para más información sobre prácticas recomendadas en la rotación de claves, véase: http://www.m3aawg.org/sites/maawg/files/news/M3AAWG_DKIM_Key_Rotation_BP-2013-12.pdf

**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); La Caixa; Message Bus; PayPal; Return Path; Time Warner Cable; Verizon Communications; y Yahoo! Inc.

**Miembros 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); McAfee Inc.; Message Systems; Mimecast; Nominum, Inc.; Proofpoint; Scality; Spamhaus; Sprint; Symantec; Trend Micro, Inc.; y Twitter.

Una lista completa de miembros está disponible en http://www.m3aawg.org/about/roster.

**Contacto con los medios:**
Linda Marcus, APR, +1-714-974-6356, LMarcus@astra.cc
Astra Communications