News Release - French

For Immediate Release

Le M³AAWG publie une nouvelle liste des meilleures pratiques pour l'implémentation de DKIM, suite à la révélation d'une vulnérabilité portant sur la longueur des clés

SAN FRANCISCO, Californie--(Marketwire - November 7, 2012) [Mise à jour : 11 décembre 2013]- Avec la possibilité récemment révélée d'envoyer des e-mails illégitimes au nom d'entreprises utilisant une clé de chiffrement expirée et faible pour l'authentification de leurs e-mails, le Groupe de travail portant sur la messagerie, les logiciels malveillants et la lutte contre l'abus mobile incite les entreprises à adapter immédiatement leurs processus DKIM (DomainKeys Identified Mail) afin d'améliorer les garanties fournies à l'utilisateur final et a publié aujourd'hui une nouvelle liste des meilleures pratiques protégeant spécifiquement contre cette vulnérabilité. Le M³AAWG appelle les entreprises à remplacer les clés de vérification de 512 et 768 bits, autrefois sécurisées, par des clés de 1 024 bits à chiffrement plus fort, entre autres recommandations destinées à mieux valider l'authenticité de l'expéditeur d'un e-mail.

« Nous avons élaboré un document bref et succinct qui explique les étapes relativement simples et immédiates que les expéditeurs peuvent suivre à grande échelle afin de protéger leur image de marque, en réponse aux préoccupations récentes concernant certains niveaux de chiffrement et d'utilisation des clés. La technologie progresse et l'industrie, pour suivre le rythme des pirates, a besoin de revoir ses pratiques à la lumière de leurs capacités croissantes. Nous voulons faire passer le mot quant aux changements rapides que les sociétés peuvent appliquer pour protéger les consommateurs et leur image de marque contre ce problème », a déclaré Chris Roosenraad, co-président du M³AAWG.

« M³AAWG Best Practices for Implementing DKIM To Avoid Key Length Vulnerability » (www.maawg.org/sites/maawg/files/news/M3AAWG_Key_Implementation_BP-2012-11.pdf) détaille les étapes techniques qui protègent contre les vulnérabilités actuelles. Ce document est disponible dans la section Published Documents du site Web de l'organisation, à l'adresse www.maawg.org/published-documents. Les recommandations comprennent :

- Mise à jour vers une clé d'une longueur minimale de 1 024 bits. Les clés plus courtes peuvent être forcées en 72 heures à l'aide de services cloud peu coûteux.
- ~~Rotation trimestrielle des clés~~ Rotation des clés au moins deux fois par an [1]
- Définition de l'expiration des signatures à l'issue de la période de rotation de la clé actuelle et révocation des anciennes clés dans le DNS.
- Utilisation du mode de test de la clé uniquement pendant une courte période de temps et retrait de la clé de test après la montée en cadence.
- Mise en œuvre de la norme DMARC (Domain-based Message Authentication, Reporting and Conformance) en mode de surveillance et utilisation du DNS pour contrôler la fréquence à laquelle les clés sont sollicitées. DMARC est une autre norme souvent utilisée en conjonction avec DKIM.
- Utilisation de DKIM plutôt que Domain Keys, qui est un protocole obsolète.
- Collaboration avec les tiers ayant été recrutés pour envoyer des e-mails au nom de la société, afin de s'assurer que ceux-ci se conforment à ces meilleures pratiques.

Largement acceptée et utilisée par les entreprises, les organismes gouvernementaux, les principaux services de fourniture de messagerie et d'autres entités, DKIM est une norme qui permet à une organisation de revendiquer la responsabilité de l'envoi d'un message, d'une manière qui peut être validée par un destinataire. Par exemple, les services de messagerie tels que AOL, Gmail et Yahoo ainsi que les marques commerciales implémentent cette norme au sein de leur protocole de messagerie. Elle inclut une clé chiffrée dans les en-têtes de message que les fournisseurs de services Internet (FSI) et d'autres destinataires utilisent pour vérifier que le message a effectivement été envoyé par la société de référence.

L'exécution de DKIM rend plus difficile pour les criminels la création de messages électroniques illégitimes conçus pour ressembler à ceux provenant d'une société reconnue, une ruse souvent utilisée pour dérober des informations personnelles sur l'identité d'utilisateurs peu méfiants. Kim Zetter, journaliste chez Wired, a signalé à la fin du mois d'octobre que de nombreuses entreprises exploitaient des clés de chiffrement faibles et employaient d'autres pratiques douteuses dans le cadre de leur mise en œuvre de DKIM, ce qui pourrait exposer leurs e-mails à cette usurpation potentielle par les cybercriminels.

[1] **NOTE** : *Quand il a été publié en 2012, le document de meilleures pratiques recommandait une rotation des clés DKIM tous les trimestres. Suite à des recherches ultérieures, donnant lieu à un nouveau document de meilleures pratiques plus détaillé sur le sujet de la rotation des clés, la recommandation sur la fréquence de rotation des clés a été mise à jour à au moins deux fois par an. Pour plus d'informations sur les meilleures pratiques concernant la rotation des clés DKIM, voir http://www.m3aawg.org/sites/maawg/files/news/M3AAWG_DKIM_Key_Rotation_BP-2013-12.pdf*

À propos du groupe de travail M³AAWG (Groupe de travail portant sur la messagerie, les logiciels malveillants et la lutte contre l'abus mobile)

Le Groupe de travail portant sur la messagerie, les logiciels malveillants et la lutte contre l'abus mobile (M³AAWG) rassemble l'industrie pour lutter ensemble contre les robots, les logiciels malveillants, les spams, les virus, les attaques par déni de service et d'autres interventions malveillantes en ligne. Le M³AAWG (www.M3AAWG.org) représente plus d'un milliard de boîtes de réception de certains des plus grands opérateurs de réseau du monde. Le groupe s'appuie sur le sérieux et l'expérience mondiale de ses membres pour s'attaquer aux abus sur les réseaux existants et dans les nouveaux services émergents en s'appuyant sur la technologie, la collaboration et les politiques publiques. Il se consacre également à la sensibilisation des décideurs mondiaux aux questions techniques et opérationnelles liées à l'abus en ligne et à la messagerie. Basé à San Francisco, en Californie, le M³AAWG est un forum ouvert axé sur les besoins du marché et soutenu par des opérateurs de réseau et des fournisseurs de messagerie de premier plan.

Conseil d'administration du **M³AAWG :** AT&T (NYSE: T), Cloudmark, Inc., Comcast (NASDAQ: CMCSA), Constant Contact (NASDAQ: CTCT), Cox Communications, Damballa, Inc., Eloqua, Facebook, France Telecom (NYSE et Euronext : FTE), La Caixa, Message Bus, PayPal, Return Path, Time Warner Cable, Verizon Communications et Yahoo! Inc.

Membres à part entière du **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. et Twitter.

Une liste complète des membres est disponible à l'adresse http://www.m3aawg.org/about/roster.

Contact auprès des médias :
Linda Marcus, APR, +1-714-974-6356, LMarcus@astra.cc
Astra Communications