News Release - For Immediate Release

Le MAAWG s'attaque aux bots avec de nouvelles lignes directrices de FAI (fournisseur d'accès Internet) pour restaurer les ordinateurs des utilisateurs finaux

SAN FRANCISCO, 3 août/PRNewswire/ - Les recommandations de l'industrie peuvent améliorer la suppression des bots pour les consommateurs

À raison du problème grandissant d'infestations de bots qui contribuent au spam du vol d'identité et de la fraude en ligne, le MAAWG (Messaging Anti-Abuse Working Group) a mis en place les premières meilleures pratiques qui visent à aider l'industrie mondiale du FAI à travailler en collaboration avec les consommateurs afin d'identifier et de supprimer les infections sur les ordinateurs des utilisateurs finaux. Le document décrit une approche à trois étapes avec des recommandations sur la détection des bots, ce qui informe les utilisateurs que leur ordinateur est compromis, et les assiste tout au long de la suppression du logiciel malveillant.

Les bots, ou logiciels malveillants, qui sont sur les ordinateurs des utilisateurs sans que ces derniers le sachent, sont responsables de 90 pour cent du spam, et peuvent également servir à voler des informations personnelles ou à prendre part à des attaques DDoS (déni de service distribué). Les meilleures pratiques courantes du MAAWG pour la limiter les infections par les bots à grande échelle dans les réseaux résidentiels (version 1.0) exposent des stratégies utilisées par certains des plus importants FAI au monde jusqu'à maintenant ont été conçues de façon à ce qu'elles soient échelonnables pour les exploitants de plus petits réseaux et pour étudier les écarts en matières judiciaires et de processus entre les pays.

« Les bots sont un fléau mondial et ces meilleures pratiques sont une étape importante de l'éducation de l'industrie sur les processus appropriés afin d'aider à protéger les consommateurs. Nous partageons les expériences de notre effectif global afin que les opérateurs de partout puissent contrer énergiquement ce problème. En tant qu'industrie, nous devenons plus proactifs à aviser les clients quand les bots sont décelés sur leur ordinateur, et à aider les utilisateurs à supprimer de logiciel malveillant avant que celui-ci fasse des ravages », explique Michael O'Reirdan, président du MAAWG.

Les nouvelles meilleures pratiques offrent différents choix d'alertes aux clients au moment où leur ordinateur devient infecté, ainsi que des suggestions pour aider les utilisateurs finaux à nettoyer leurs systèmes. Le document présente des méthodes de détection de bots, des avertissements au client, ainsi que des jardins fermés pour limiter l'exposition des ordinateurs infectés à Internet. Parmi ces recommandations :

- Tout en protégeant la vie privée de l'utilisateur, les exploitants de réseau peuvent utiliser différents outils pour détecter les ordinateurs infectés des utilisateurs finaux, comme le DNS, le scannage de l'espace IP pour identifier les ordinateurs vulnérables, et la collecte d'information IP sur le trafic pour les opérations connues et les lieux de contrôle.

- Les emails, les appels téléphoniques aux clients, le courrier par la poste et les jardins fermés sont des outils d'avertissement fréquemment utilisés, chacun ayant ses propres considérations. La messagerie par navigateur est considérée comme la méthode la plus efficace pour alerter les clients, mais elle peut cependant être techniquement difficile à implanter.

- Les FAI doivent soutenir une sécurité de portail bien annoncée qui comprend de directives pour la suppression de bots par les utilisateurs.

Le document comprend aussi des échantillons de messages d'utilisateurs finaux et une liste de détection de logiciels malveillants et d'outils de suppression. Les meilleures pratiques continueront de faire l'objet de révision afin de refléter les nouvelles procédures et l'évolution de nouvelles menaces de bots.

Les utilisateurs sous-estiment la menace bot

Un bot qui est logé sur l'ordinateur d'un consommateur fait généralement partie d'un plus grand réseau d'ordinateurs programmés pour performer des opérations spécifiques et clandestines sous le contrôle d'un « maître de bot ». Le logiciel malveillant est fréquemment installé sur des ordinateurs de consommateurs peu méfiants, lorsque ces derniers cliquent sur un email infecté ou téléchargent des codes illicites de sites Web compromis. Les bots sont conçu pour agir discrètement, par exemple en envoyant du spam ou en enregistrant des mots de passe et des informations personnelles sans la connaissance des propriétaires - ce qui rend difficile pour les utilisateurs finaux de les détecter sur leurs ordinateurs infectés.

Alors qu'environ 80 pour cent des consommateurs connaissent l'existence des bots, seulement 20 pour cent croient qu'ils ne seront pas infectés, selon un sondage du MAAWG publié en juillet (le sondage et autres communiqués de presse sur le sujet sont disponibles sur le site www.MAAWG.org). « Les FAI doivent franchir les étapes afin de protéger les utilisateurs, mais nous avons aussi besoin d'éduquer constamment les clients et travailler ensemble à localiser la propagation de bots », affirme M. O'Reirdan.

Les nouvelles meilleures pratiques d'atténuation font partie du travail de MAAWG qui consiste à combattre l'abus de messages. Antérieurement, MAAWG a publié les meilleures pratiques pour la gestion du port 25, en utilisant des jardins fermés avec un espace dynamique d'adresse IP, des procédures de réacheminement d'emails, et des procédures de meilleures communications d'expéditeurs, entre autres.

Les meilleures pratiques fréquentes du MAAWG pour l'atténuation des infections bot à grande échelle dans les réseaux résidentiels peuvent être téléchargées à partir du site Web de l'organisation au www.MAAWG.org. Le sondage auprès des consommateurs du MAAWG a publié des livres blancs qui sont également disponibles sur le site.

À propos du Messaging Anti-Abuse Working Group (MAAWG)

Le Messaging Anti-Abuse Working Group (MAAWG) (Groupe de travail contre les abus de messagerie électronique) est le point de rencontre des professionnels de l'industrie qui souhaitent lutter contre le spam, les virus, les attaques de refus de service et d'autres formes de malveillance en ligne. Le MAAWG (www.MAAWG.org) représente près d'un milliard de boîtes aux lettres électroniques de certains des plus grands opérateurs de réseau dans le monde. Il s'agit de la seule organisation apportant une réponse globale aux messages indésirables en traitant systématiquement tous les aspects du problème, notamment la technologie, la collaboration sectorielle et la politique publique. Le MAAWG mise sur l'importance et l'expérience de ces membres à l'échelle mondiale pour combattre l'abus des réseaux existants et des nouveaux services émergents. Basée à San Francisco, en Californie, le MAAWG est un forum ouvert s'adaptant aux besoins du marché et soutenu par les principaux opérateurs de réseau et fournisseurs de messagerie.

-30 -

Linda Marcus, agente de relations publiques chez Astra Communications, +1-714-974-6356, lmarcus@astra.cc

Conseil d'administration du MAAWG : AOL, AT&T (NYSE : T), Cloudmark, Inc., Comcast (Nasdaq : CMCSA), Cox Communications, France Télécom (NYSE et Euronext : FTE), Goodmail Systems, Openwave Systems (Nasdaq : OPWV), Time Warner Cable, Verizon Communications, et Yahoo! Inc.

Membres à part entière du MAAWG : 1&1 Internet AG, Bizanga LTD, Constant Contact, e-Dialog, Eloqua Corporation, Experian CheetahMail, Genius.com, Internet Initiative Japan, (IIJ Nasdaq : IIJI), IronPort Systems, McAfee Inc., MX Logic, NeuStar, Inc., Outblaze LTD, Return Path, Inc., Spamhaus, Sprint, et Symantec

Une liste complète des membres est disponible au http://www.maawg.org/about/roster.