News Release - For Immediate Release

MAAWG geht mit neuen ISP-Richtlinien für die Wiederherstellung infizierter Endanwendermaschinen gegen Bots vor

SAN FRANCISCO, 3. August/PRNewswire/ -- Die Branchenempfehlungen unterstützen den Verbraucher bei der Beseitigung von Bots

Angesichts des zunehmenden Problems des Bot-Befalls, der zu Spam, Identitätsdiebstahl und Onlinebetrug beiträgt, hat die MAAWG (Messaging Anti-Abuse Working Group) erstmals optimale Praktiken herausgegeben, die die weltweite ISP-Branche dabei unterstützen sollen, mit dem Verbraucher bei der Erkennung und Beseitigung von Bot-Infektionen auf Endanwendermaschinen enger zusammenzuarbeiten. In dem Artikel wird ein dreistufiger Ansatz verfolgt und Empfehlungen zur Entdeckung von Bots, zur Benachrichtigung des Anwenders über den Befall und zur Hilfestellungen bei der Beseitigung der Malware gegeben.

Bots bzw. Schadprogramme, die auf dem Computer des Anwenders ohne dessen Wissen ablaufen, sind für bis zu 90% aller Spams verantwortlich und werden auch eingesetzt, um persönliche Informationen zu entwenden bzw. für DDoS-Angriffe (Distributed Denial of Service) genutzt. Der Artikel mit dem Titel „MAAWG Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks (Version 1.0)“ (Allgemeine optimale Praktiken der MAAWG zur Verhinderung weitreichender Infektionen in Heim-Netzwerken) erläutert die Strategie, die von einigen der größten ISPs weltweit eingesetzt werden. Diese sind jedoch so konzipiert, dass sie auch für kleinere Netzwerkbetreiber herunterskaliert werden können und die rechtlichen und verfahrenstechnischen Unterschiede in den verschiedenen Ländern berücksichtigen.

„Bots sind ein weltweites Problem und diese optimalen Praktiken sind ein wichtiger Schritt, um die Branche auf die passenden Verfahren aufmerksam zu machen, mit denen sie den Verbraucher schützen können. Wir geben auf diese Weise die Erfahrungen unserer weltweiten Mitglieder weiter, so dass Netzwerkbetreiber überall auf der Welt dieses Problem offensiv angehen können. Wir werden als Branche zunehmend vorbeugend tätig und warnen Kunden, sobald wir Bots auf ihren Computern entdecken und helfen ihnen, die Schadprogramme zu beseitigen, bevor diese Schaden anrichten können“, sagte Michael O'Reirdan, Vorsitzender der MAAWG.

In den neuen optimalen Praktiken werden zahlreiche Möglichkeiten aufgezeigt, wie man Kunden darauf aufmerksam machen kann, dass ihr Computer infiziert ist. Des Weiteren enthalten sie Vorschläge, wie dem Endanwender bei der Säuberung seines Systems geholfen werden kann. Der Artikel erläutert Bot-Erkennungsverfahren, Kundenbenachrichtigung und den Einsatz so genannter „Walled Gardens“, die eine infizierte Maschine vom Internet abgrenzen. Hier einige Empfehlungen:

- Ohne Einschränkung des Datenschutzes kann der Netzwerkbetreiber zahlreiche Hilfsmittel einsetzen, um infizierte Endanwendercomputer ausfindig zu machen, unter anderem über die DNS und das Absuchen des IP-Raumes, um anfällige Computer zu identifizieren und Informationen über den IP-Verkehr bekannter Befehls- und Steuerungsadressen zu erfassen.

- E-Mail, Anrufe beim Kunden, Briefe und Walled Gardens sind die Hilfsmittel der Wahl, um den Anwender zu benachrichtigen, wobei jedes dieser Mittel ganz eigene Überlegungen erfordert. Direktmeldungen im Browser gelten als

das wirksamste Verfahren, um den Kunden zu warnen, sind aber technisch nicht immer ganz leicht zu implementieren.

- ISPs sollten ein gut sichtbares Sicherheitsportal betreiben, auf dem der Endanwender Anweisungen für die Beseitigung von Bots findet.

Der Artikel enthält auch Musterbeispiele für die Benachrichtigung des Endanwenders und eine Liste der Tools zur Erkennung und Beseitigung von Schadprogrammen. Die optimalen Praktiken werden laufend aktualisiert, um mit neuesten Verfahren und der Entwicklung neuer Gefahren durch Bots Schritt halten zu können.

Anwender unterschätzen die Gefährlichkeit von Bots

Ein auf einem Endanwendercomputer befindlicher Bot ist üblicherweise Teil eines größeren Netzwerks, das darauf programmiert ist, im Verborgenen ganz bestimmte Aufgaben unter der Aufsicht eines „Botmasters“ durchzuführen. Die Schadprogramme werden häufig auf den Maschinen ahnungsloser Verbraucher installiert, wenn diese auf eine infizierte E-Mail klicken bzw. rechtswidrige Programme von einer kompromittierten Website herunterladen. Bots sind so konzipiert, dass sie heimlich betrieben werden und z.B. Spam verschicken oder Passwörter und persönliche Angaben ohne Wissen des Besitzers aufzeichnen. Dies macht es für den Endanwender sehr schwer, festzustellen, ob seine Maschine infiziert ist.

Während sich ca. 80 Prozent der Verbraucher der Bots-Gefahr durchaus bewusst sind, glauben nur 20 Prozent, selbst infiziert werden zu können, so das Ergebnis einer im Juli von der MAAWG durchgeführten Umfrage (die Umfrage und die entsprechende Pressemitteilung stehen unter www.MAAWG.org zur Verfügung). „ISPs müssen zwar Maßnahmen zum Schutz des Anwenders ergreifen, aber wir müssen den Kunden auch laufend aufklären und eng mit ihm zusammenarbeiten, um der Verbreitung von Bots Einhalt zu gebieten“, sagte O'Reirdan.

Die neuen optimalen Praktiken zur Schadensminderung durch Bots sind Teil des laufenden Kampfes der MAAWG gegen Messaging-Missbrauch. Zu einem früheren Zeitpunkt hatte die MAAWG bereits u. a. optimale Praktiken zur Handhabung des Ports 25, zum Einsatz von „Walled Gardens“, zur gemeinsamen Nutzung dynamischer IP-Adressräume, zur Weiterreichung von E-Mails und zur Kommunikationspraxis für Massenversender herausgegeben.

Die allgemeinen optimalen Praktiken der MAAWG zur Verhinderung weitreichender Bot-Infektionen in Heim-Netzwerken (MAAWG Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks) können auf der Website der Organisation unter www.MAAWG.org heruntergeladen werden. Dort stehen auch die Kundenumfrage der MAAWG, die bereits herausgegebenen Weißbücher und optimalen Praktiken zur Verfügung.

Informationen zur MAAWG-Arbeitsgruppe (Messaging Anti-Abuse Working Group)

In der Messaging Anti-Abuse Working Group (MAAWG) hat sich die Messaging-Branche vereint, um gemeinsam gegen Spam, Viren, Denial-of-Service-Attacken und andere Formen des Online-Missbrauchs zu kämpfen. Die MAAWG (www.MAAWG.org) vertritt nahezu eine Milliarde Posteingangsfächer einiger der weltweit größten Netzwerkbetreiber. Es handelt sich um die einzige Organisation, die ganzheitlich auf Messaging-Missbrauch eingeht und systematisch alle Aspekte des Problems, u. a. technologische Gesichtspunkte sowie Fragen der Kooperation innerhalb der Branche und mit den öffentlichen Entscheidungsträgern abgedeckt. Die MAAWG nutzt die gemeinsamen Erfahrungen ihrer weltweiten Mitglieder, um den Missbrauch in bestehenden Netzwerke und bei neuen, aufkommenden Diensten zu unterbinden. Die MAAWG hat ihren Hauptsitz in San Francisco (Kalifornien) und biete ein offenes Forum, das von den Anforderungen des Markts getragen und von bedeutenden Netzwerkbetreibern und Messaging-Anbietern unterstützt wird.

-30-

Linda Marcus, APR von Astra Communications, Tel.: +1-714-974-6356, E-Mail: lmarcus@astra.cc

Folgende Unternehmen bilden den Vorstand der MAAWG: AOL, AT&T (NYSE: T), Cloudmark, Inc., Comcast (Nasdaq: CMCSA), Cox Communications, France Telecom (NYSE und Euronext: FTE), Goodmail Systems, Openwave Systems (Nasdaq: OPWV), Time Warner Cable, Verizon Communications und Yahoo! Inc.

Folgende Unternehmen sind Vollmitglieder der 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 und Symantec

Die komplette Mitgliedsliste steht unter http://www.maawg.org/about/roster zur Verfügung \.