M3AAWG
MESSAGING MALWARE MOBILE

To: **U.S. Federal Communications Commission**
From: **Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG)**
Date: **September 26, 2014**
Subject: **Comments on Implementation of CSRIC III Cybersecurity Best Practices**

Thank you for the opportunity to submit comments on the implementation status of the FCC's CSRIC III Cybersecurity Best Practices.

The Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) is an international non-profit industry-led organization founded to fight all forms of abuse, such as phishing, botnets, fraud, spam, viruses and denial-of-service attacks. M^{3}AAWG draws technical experts, researchers and policy specialists from a broad base of Internet service providers and network operators representing over one billion mailboxes, as well as from key technology providers, academia and volume sender organizations. The multidisciplinary approach at M^{3}AAWG (www.m3aawg.org) includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards, and the facilitation of collaboration.

Among other questions, your notice invited commenting parties to address the implementation and effectiveness of the CSRIC III recommendations including the Anti-Bot Code of Conduct that was developed as part of CSRIC III Working Group #7 chaired by M^{3}AAWG Chairman Emeritus Michael O'Reirdan. The Anti-Bot Code of Conduct calls for ISPs to take "meaningful action" in each of five areas: Education, Detection, Notification, Remediation and Collaboration. M^{3}AAWG has promoted this effort with a dedicated page on our website listing companies that support the code (www.m3aawg.org/abcs-for-ISP-code). We have also linked videos on this page from our public YouTube channel (www.youtube.com/maawg) explaining the importance of the code and a training session from a M^{3}AAWG General Meeting where a network security expert explains how ISPs can implement the code.

Since the publication of the Anti-Bot Code of Conduct, M^{3}AAWG has undertaken an initiative to develop metrics, including data provided directly by ISPs and network operators, that examines the level of bot infections on consumer networks and the percentage of subscribers notified their systems were affected. This is the first cooperative effort by the network companies that directly provide end-users Internet access, and thus see the data first hand, to quantify the extent of malicious bots afflicting their subscribers.

The report shown on page 3 of these comments covers up to 43.5 million consumer subscribers in Europe and North America. Based on the data provided to M^{3}AAWG, in 2012 participating network operators reported the number of infected subscribers ranged from .84% to 1.8% with 99.13% to 99.21% of those subscribers being notified they had a bot. In 2013, the number of infected subscribers varied from slightly over 1% to .80% with 99.82 to slightly under 94% of consumers being notified.

About the M^{3}AAWG Bot Metrics Program

This is a voluntary program of data provided confidentially by ISPs and network operators who are working within M^{3}AAWG to address malware and bots. It covers only end-user connections and does not include enterprise business networks. The data is shared at the discretion of each company and is reported here as aggregated metrics and thus represents the contributions of participating ISPs. M^{3}AAWG members are under no obligation to supply this information or to participate in this program.

This cooperative effort was organized as an objective tool for tracking industry and government efforts at controlling the spread of bots. M^{3}AAWG network operator members have invested over a year of their time and effort to developing these pilot metrics, and we are committed to continuing this important work. Similar to the M^{3}AAWG Email Metrics Report on abusive messaging, we expect these reports will become an important resource for understanding the extent of bot infections and to measuring the effectiveness of the industry's efforts to protect end-users.

Observations

While definitions of bots can differ from country to country, the metrics below report on malware, or malicious code, discovered by a network operator while processing a subscriber's email or other Internet activities. Bots are installed directly on end-users' systems, often without their knowledge. Once deployed, the "botted" machine can be controlled by commands from a "bot master," a person who uses infected machines as a network to send spam or carry out fraudulent activities. The malicious code is often designed to run in background mode, so subscribers are usually unaware their systems are infected.

While Internet service providers and network operators are able to identify infected users on their networks, subscribers must remove the malware from their systems. Based on the data in this report, network operators are notifying about 98.7% of end-users when they are infected. This points out the importance of the entire Internet ecosystem working together to address this problem, including security software vendors and end users.

M^{3}AAWG is planning to continue updating this data to further analyze this issue. There also may be an opportunity for this project to examine the responsiveness or effectiveness of notifications from an end user perspective. This is a more complicated question that involves the entire ecosystem beyond ISPs and may reveal lessons learned from different communications techniques employed by varying operators to notify end users. This is an issue that M^{3}AAWG may consider analyzing more thoroughly in 2015, in addition to updating the current metrics.

Thank you for the opportunity to submit these comments. As noted, please see the attached M^{3}AAWG Bot Metrics Report dated September 24, 2014 on page 3. We will be glad to respond to any questions. Please address any inquiries about our work to me, M^{3}AAWG Executive Director Jerry Upton, at jerry.upton@m3aawg.org.

Sincerely,
Jerry Upton, M^{3}AAWG Executive Director
Jerry.Upton@m3aawg.org

M^{3}AAWG Bot Metrics Report

September 24, 2014

The statistics reported below are compiled from confidential monthly data provided by participating M^{3}AAWG member ISPs and network operators summarized here by quarter from 2012 through 2013. Our reporting basis covers a quarterly average of up to 43.5 million subscribers.

2012	Q1 2012	Q2 2012	Q3 2012	Q4 2012
Subscribers Represented	37,707,435	37,358,206	36,991,516	37,383,662
Subscribers Deemed Infected	317,064	402,585	249,492	440,746
% Infected	0.84%	1.08%	0.67%	1.18%
Infected Subscribers Notified	314,295	400,439	245,522	437,253
% Notified	99.13%	99.47%	98.41%	99.21%

2013	Q1 2013	Q2 2013	Q3 2013	Q4 2013
Subscribers Represented	37,270,265	37,735,195	37,639,022	43,550,674
Subscribers Deemed Infected	388,152	435,921	493,572	346,615
% Infected	1.04%	1.16%	1.31%	0.80%
Infected Subscribers Notified	387,221	435,149	492,382	325,787
% Notified	99.76%	99.82%	99.76%	93.99%

What is Measured?

- **Number of Subscribers**
  The number of specific subscribers on a network. Each subscriber may represent more than one end-user or include multiple devices.
- **Infected Subscribers**
  This is the count of unique subscribers identified to be infected in each reporting period.
- **Percent of Base Infected**
  Calculated from above: Infected Subscribers divided by Number of Subscribers
- **Total Number of Infected Subscribers Notified**
  The number of unique subscribers notified of a bot by any method, including text message, phone call, email, web redirection or browser notification, and postal mail. Multiple notices sent to the same subscriber are counted as one. This does not imply that the subscriber received or read the notice.
- **Percent Notified**
  Calculated from above: Infected Subscribers Notified / Infected Subscribers